

Integrated Safeguards and Security Management Self-Assessment 2002

Suzanne Bowen, Dwayne Ramsey, James Rothfuss,
Dennis Hall, Erik Richman, and John Hules

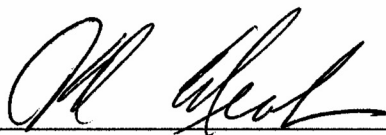
Ernest Orlando Lawrence Berkeley National Laboratory
Berkeley, CA 94720

August 2003

Approved by:



D. C. McGraw
Division Director
Environment, Health and Safety Division



A. X. Merola
Division Director
Information Technologies and Services Division

This work was supported by the Director, Office of Science, of the U.S. Department of Energy
under Contract No. DE-AC03-76SF00098.

Contents

Executive Summary	1
Integrated Safeguards and Security Management Self-Assessment 2002	3
Purpose of the ISSM Self-Assessment	4
ISSM Self-Assessment Process and Results	4
Development and Implementation of the Self-Assessment Process	4
Employee Survey	6
Cyber and Physical Security Data	7
Organizational Profiles and Institutional Matrix	7
Continuous Improvement Plan	8
Immediate Improvements	8
Security Baseline and Future Improvements	8
Assurance Provided	9
Improvement of the Self-Assessment Process	14
Improvement of the Laboratory's Security Program	15
Improvement of Related Lab-Wide Processes	17
Action Items	18
Line Management	18
ISSM Staff	19
Appendix A: Integrated Safeguards and Security Management Plan	A-1
Appendix B: Self-Assessment Questionnaire	B-1
Appendix C: Detailed Survey Results	C-1
Appendix D: Performance Rating Criteria	D-1
Appendix E: Organizational Profiles	E-1
Appendix F: Institutional Profiles	F-1

Integrated Safeguards and Security Management Self-Assessment 2002

Executive Summary

In 2002 Ernest Orlando Lawrence Berkeley National Laboratory developed and deployed an Integrated Safeguards and Security Management (ISSM) Self-Assessment process to measure how well the Laboratory's 2001 ISSM Plan has been implemented. The cornerstone of the Self-Assessment is an employee survey that was designed to meet several objectives:

- provide a baseline measurement of the Laboratory's current security status and ensure that Laboratory assets are protected
- educate all Laboratory staff about security responsibilities, tools, and practices
- provide security staff with feedback on the effectiveness of security programs
- provide line management with the information they need to make informed decisions about security.

Every employee received an information packet and instructions for completing the ISSM survey in September 2002. The survey contained questions designed to measure awareness and conformance to policy and best practices. The survey response Lab-wide was excellent — 88% of lab employees completed the questionnaire. ISSM liaisons from each division followed up on the initial survey results with individual employees to improve awareness and resolve ambiguities uncovered by the questionnaire. Thus the Self-Assessment produced immediate positive results for the ISSM program and revealed opportunities for longer-term corrective actions.

Results of the questionnaire were combined with institutional data from the physical and cyber security staff to provide organizational profiles and an institutional summary. The overall level of security protection and awareness was very high — often above 90%. Post-survey work by the ISSM liaisons and line management consistently led to improved awareness and metrics, as shown by a comparison of profiles at the end of phase one (October 29, 2002) and phase two (February 19, 2003). The Self-Assessment confirmed that classified information and DOE sensitive information are not held or processed at Berkeley Lab. The questionnaire also provided the first systematic listing of assets and information that staff felt required extra protection, which can be vetted against existing countermeasures. In addition, the survey results identified some information and processes requiring increased employee knowledge and awareness. Line management will be able to determine additional corrective actions based on the results of the Self-Assessment.

Future assessments will raise the ratings bar for some existing program elements and add new elements to stimulate further improvements in Laboratory security.

Integrated Safeguards and Security Management Self-Assessment 2002

In April 2001 Berkeley Lab adopted its Integrated Safeguards and Security Management (ISSM) Plan¹ to integrate all aspects of security into the fabric of Laboratory operations. The plan outlines the Berkeley Lab ISSM program, which is designed to ensure the protection of Berkeley Lab assets, including physical and intellectual property, and is closely aligned with DOE P 470.1, *Integrated Safeguards and Security Management (ISSM) Policy*.

The vision and mission of the ISSM Plan are:

Vision

Integrated security supports and protects innovative science.

Mission

The Berkeley Lab Security program assures all visitors and employees of an open and secure work environment that fosters the continuation of creative scientific advances. Integrated security management ensures the protection of Laboratory assets, including physical and intellectual property, and establishes programs for cyber security, export control and counterintelligence.

Six guiding principles and five security functions were developed to form the core of ISSM:

Guiding principles

1. Line management owns security.
2. Clear roles and responsibilities are defined and communicated.
3. Cyber and physical security, export control management, and counterintelligence functions are integrated.
4. An open environment supports the Berkeley Lab mission.
5. Security is a value-added activity supporting research and support operations.
6. Security controls are tailored to individual and facility requirements.

Security functions at an institutional level

1. Work planning. The tasks to be accomplished as part of any given activity are defined clearly.
2. Analyze threats to the extent possible.
3. Develop appropriate countermeasures to threats, and communicate information regarding threats, countermeasures, and controls.

¹ The ISSM Plan is included in Appendix A and is available on the Web at <http://www.lbl.gov/ehs/security/issm/ISSMfinal.html>.

4. Perform work within the controls.
5. Continuous feedback.

Purpose of the ISSM Self-Assessment

After adoption of the ISSM Plan, line management asked that an assessment mechanism be developed to measure how well the plan has been implemented. The Self-Assessment was designed to provide a baseline measurement of the Laboratory's current security status and to ensure that Laboratory assets are protected; to educate staff about security responsibilities, tools, and practices; to provide security staff with feedback on the effectiveness of security programs; and to provide line management with the information they need to make informed decisions about security.

The specific purpose of the first Self-Assessment for 2002 was to develop and administer the Self-Assessment process, making it a smooth process that can be easily modified to lead to significant improvements in the future. The difficulty of the questions and the rating criteria will increase in subsequent years to reflect incremental improvements each year.

ISSM Self-Assessment Process and Results

In September 2002 Berkeley Lab began the ISSM Self-Assessment process. ISSM liaisons were designated for each organization at the Laboratory to represent line management during the process. The Self-Assessment included an all-employee survey and both rated and non-rated data maintained by the physical and cyber security staff. Results were provided to line managers in the form of organizational profiles and an institutional report, which together identify unmitigated risks in order to improve ISSM performance in specific areas and to evaluate the overall ISSM program. All of these components were developed into a Web-based system that can be easily be managed and updated for future Self-Assessments (Figure 1).

Development and Implementation of the Self-Assessment Process

The ISSM Self-Assessment was developed and implemented in the following steps:

- Self-Assessment commissioned.
- Approach developed and presented to David McGraw, Director of the Environmental Health and Safety Division (EHS), and Sandy Merola, Chief Information Officer and Director of the Information Technologies and Services Division (ITSD).
- Self-Assessment process presented to Deputy Director for Operations Sally Benson.
- Prototype Web-based survey and profiles developed.
- ITSD and EHS used as "test divisions" to test prototype process.
- Improvements made.
- Self-Assessment process presented to division directors and given go-ahead.
- Survey started.

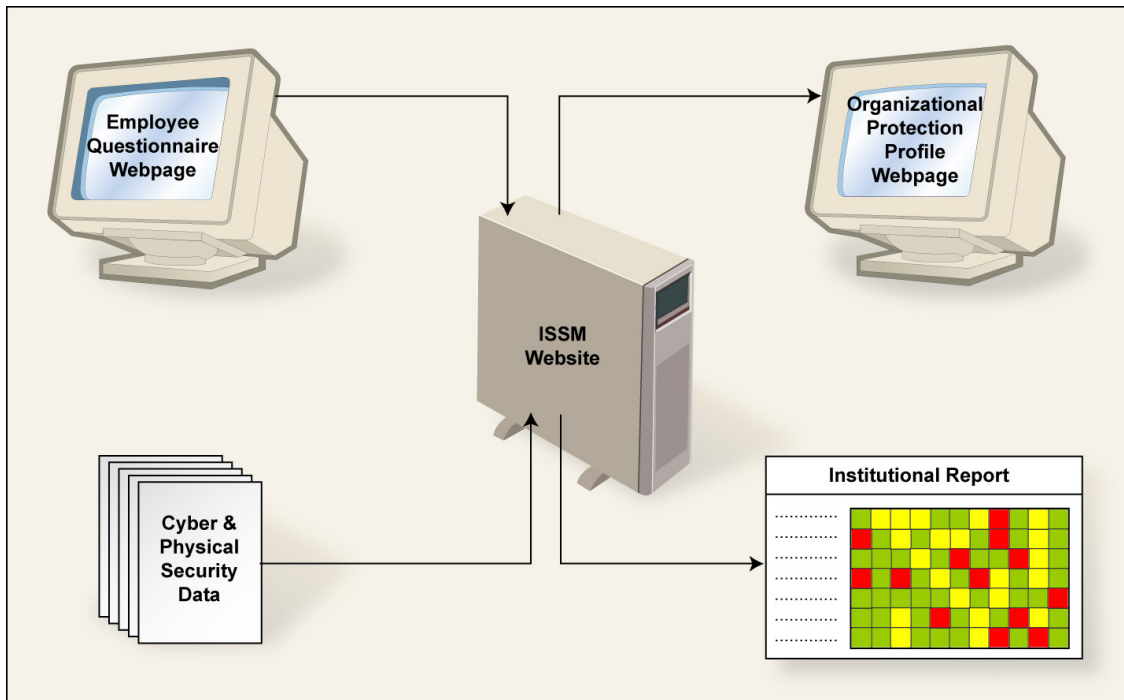


Figure 1. ISSM Self-Assessment components.

- Results for each organization opened to division and organization directors and ISSM security liaisons.
- ISSM security liaisons followed up on survey results.
- Improvements to survey results officially closed.
- ISSM Self-Assessment Report (this document) submitted.

The Self-Assessment measures the Laboratory against several of the ISSM principles and functions:

- *Line management owns security*: The organizational profiles give the division directors and other managers the information they need to make informed decisions and improvements.
- *All security functions are integrated*: This is the first effort since the conception of ISSM in which all security functions (physical, personnel, cyber, export control, counter-intelligence) are encompassed in one project.
- *Clear roles and responsibilities*: The questionnaire and organizational profiles reinforce each individual's responsibilities and gives them the means to learn more about those responsibilities.
- *Define security elements and threats*: The Self-Assessment collects data from the security programs and individual employees that can be used to assess threat and risk to the Laboratory.
- *Perform work within the controls*: The Self-Assessment measures performance data that can be used for immediate control improvements and to identify future areas for performance improvement.

- *Continuous feedback:* The Self-Assessment provides data for identifying weaknesses and measuring improvement.

The feedback loops in the Self-Assessment process (Figure 2) are designed to stimulate both short- and long-term improvements in security.

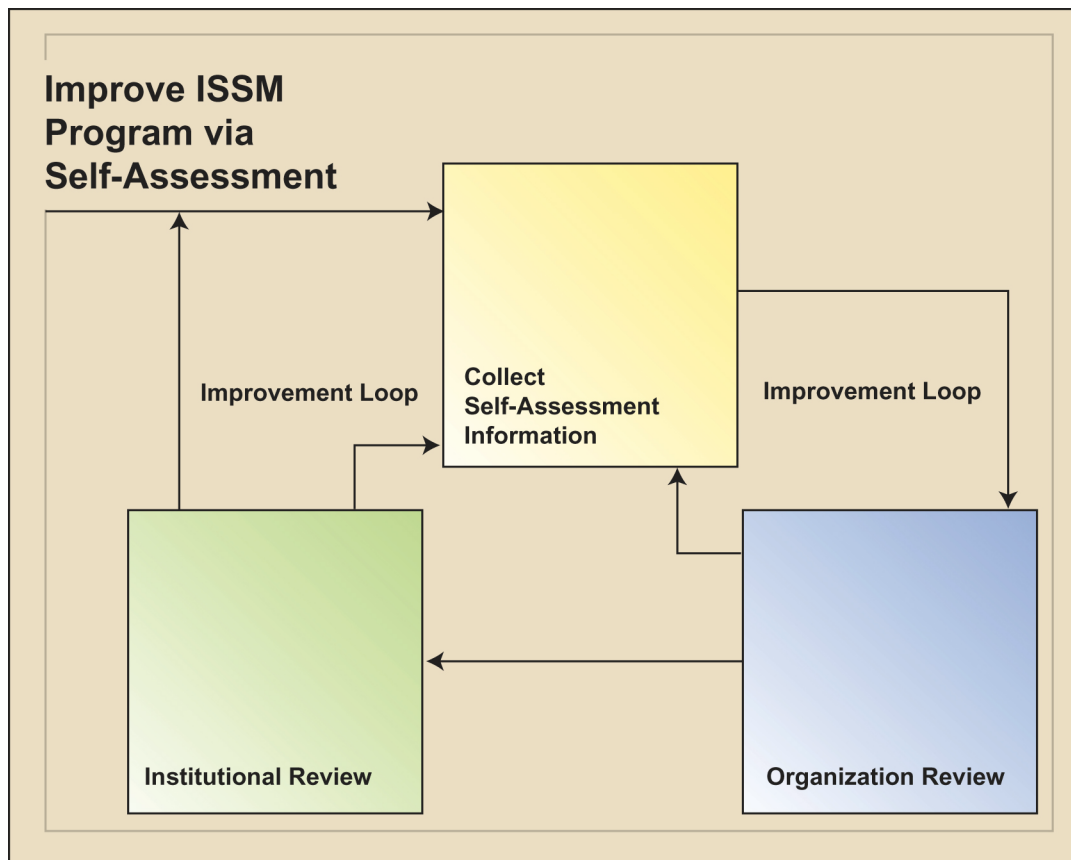


Figure 2. ISSM Self-Assessment process.

Employee Survey

The Self-Assessment began in early September when every employee was sent a packet of information that included the employee guide *Security at Berkeley Lab*, a computer security banner, and instructions for completing the ISSM survey. The survey was also publicized in the employee newspaper *Currents* and in the weekly email newsletter *Headlines*. On September 9, a Level 1 email was also sent to all employees requesting their participation in the ISSM survey. Employees were encouraged to complete the survey during the next three weeks, concluding the process on September 27, 2002.

The employee survey (Appendix B) was designed as a tool, not a test. It was intended to gather baseline data to document the laboratory's current security status, and also to educate employees about security. Care was taken to make the survey easy and quick. The survey questions were very carefully chosen to be both relevant and simple, and the

number of questions was limited to 18. The survey was designed primarily as a Web-based questionnaire, and hyperlinks were provided to assist staff in finding the information they needed to answer the questions correctly. A paper version of the survey was supplied to staff who do not have regular access to a computer. The survey was designed to be easily modified in the future to assess other target areas.

After September 27, when the initial survey phase of the Self-Assessment was completed, the ISSM liaisons were encouraged to examine the initial results for their organization and to follow up on the survey results with individual employees to improve awareness, resolve ambiguities, and remedy any problems uncovered by the questionnaire. Employees who had not participated in the survey were contacted and encouraged to complete the survey. This process continued until the division and organization directors reviewed their results in January 2003. The organization results were finalized on February 19, 2003.

The success of the employee survey exceeded expectations. In all, 3,551 staff completed the survey (88%). This high rate of participation suggests a high level of awareness and commitment to security at the Laboratory. No significant technical problems in the survey process were reported. There was minimal need for individual help in completing the survey. Survey participants contributed about 250 helpful suggestions for improving the survey. Detailed results of the employee survey are provided in Appendix C.

Cyber and Physical Security Data

A second source of information for the Self-Assessment was statistical data provided by the physical and cyber security staff regarding computer system vulnerabilities, cracked passwords, and thefts. This information complements the survey results, giving a more complete picture of organizational performance.

Organizational Profiles and Institutional Matrix

Results from the employee survey were combined with the cyber and physical security data to create organizational profiles for each Laboratory division and organization. Some results were given a rating of green, yellow, or red to give managers an indication of the level of performance. The rating criteria (Appendix D) were designed to be realistic and attainable. The organizational profiles (Appendix E) are also Web-based and are designed to be updated automatically with the latest survey results.

The institutional matrix (Appendix F) is a Web-based, color-coded chart that summarizes all the organizational profiles, giving a quick picture of the Laboratory's overall performance. The survey results reflected increased employee knowledge and awareness of security issues, and identified information and processes requiring higher levels of protection, as discussed below.

Continuous Improvement Plan

By giving management the information needed to make informed decisions about security, the ISSM Self-Assessment promotes both short- and long-term improvements. This section discusses already realized or potential improvements resulting from the 2002 Self-Assessment.

Immediate Improvements

The organizational review and follow-ups of the ISSM security liaisons to the initial staff survey results produced immediate improvements in the organization and institutional profiles. The total number of red ratings was reduced by 95%, while the yellow ratings were reduced by 53% (Figure 3 and Appendix F).

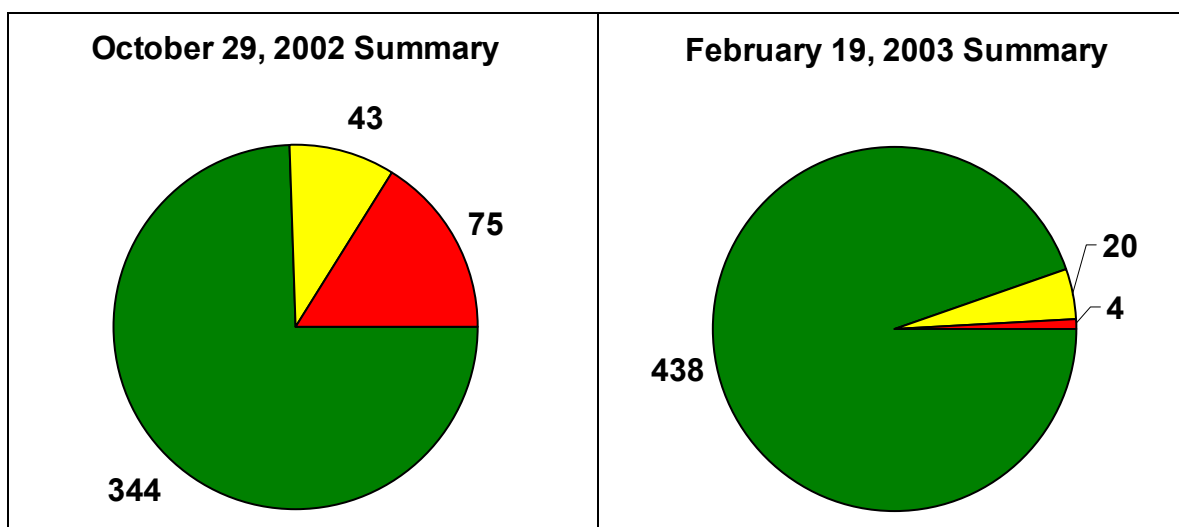


Figure 3. Institutional profile improvements resulting from organizational review and security liaison follow-ups (22 organizations × 21 metrics).

The organizational review and security liaison follow-ups resulted in many improvements, including:

- Understanding of policy regarding legal software improved 10%.
- Cracked passwords on central servers decreased from 772 to 10 during the assessment period.
- Scanned vulnerabilities of high-risk computers decreased from 1,669 to 2 during the assessment period.

Details regarding these and other improvements can be found in Appendices C and E.

Security Baseline and Future Improvements

The 2002 ISSM Self-Assessment has set a baseline for Berkeley Lab security, with assurance that selected security parameters have been verified. The Self-Assessment also identified areas needing improvement. This section of the report discusses specific Self-Assessment results organized in the following categories:

- assurance provided
- improvement of the Self-Assessment process
- improvement of the Laboratory's security program
- improvement of related Lab-wide processes.

Assurance Provided

The Self-Assessment provides management with a high degree of assurance that the Laboratory is secure with respect to information security, system protection, cyber security, physical protection, and general security awareness. These results are discussed in detail below.

INFORMATION SECURITY

The questionnaire posed a series of inquiries about classified and DOE-sensitive information created or processed at Berkeley Lab. DOE-sensitive information includes Unclassified Controlled Nuclear Information (UCNI) and Naval Nuclear Propulsion Information (NNPI). Classified and DOE-sensitive information are not allowed at Berkeley Lab, so these questions provide assurance that these prohibitions are understood and are being followed.

Clearance Holders. Although no classified information is allowed at Berkeley Lab, a number of LBNL staff hold security clearances issued by DOE and other federal entities. There is no agency that can provide LBNL with a comprehensive list of these clearance holders. In the past, periodic requests to staff have been used to develop a list of LBNL clearance holders. Capturing all security clearance holder employees in our database was an important aspect of the Self-Assessment. At the time the Self-Assessment was conducted, DOE required that laboratories track all clearance-holder employees who host foreign nationals from sensitive countries.² The ISSM Self-Assessment accomplished this goal by identifying additional employees and guests who hold security clearances from other facilities. A more comprehensive list of clearance holders gleaned by this survey has been given to the Laboratory's counterintelligence officer for follow-up.

Classified Information. The first Self-Assessment question to staff was "Do you work with classified information³ at LBNL?" In the initial answers of 3,473 respondents, 17 stated that they worked with classified information. The division ISSM liaisons contacted these respondents and determined that none work on classified information at LBNL. While some LBNL staff do, in fact, work with classified material at other facilities, most of the erroneous answers came from a misunderstanding of the definition of classified information. It is significant that a very small number of those surveyed believed that they work with classified information at LBNL and that their mistaken understanding was corrected during the Self-Assessment.

² DOE N 142.1, Unclassified Foreign Visits and Assignments, July 14, 1999.

³ Staff were provided with hyperlinks (underlined in this report) to the appropriate definitions and other information.

Unclassified Controlled Nuclear Information (UCNI). All staff were asked, “Do you work with UCNI at LBNL?” Of 3,473 initial respondents to the questionnaire, only 13 responded affirmatively. Investigation by the ISSM liaisons determined that none of the affirmative responses were correct. As in the case of classified information, the responses were prompted by a lack of understanding of the definition of UCNI.

Naval Nuclear Propulsion Information (NNPI). All staff were asked “Do you work with NNPI at LBNL?” Of 3,473 initial respondents to the questionnaire, only seven responded affirmatively. Investigation by the ISSM liaisons determined that none of the affirmative responses were correct. Again the erroneous initial responses were prompted by a lack of understanding of the definition of NNPI.

SYSTEM PROTECTION

The Berkeley Lab protective programs are based on the premise that the Laboratory is operated largely as an open environment and the information and systems that need extra protection are given appropriate attention. The Self-Assessment asked a series of questions designed to elicit this type of information. The first questions dealt with the type of information being processed (proprietary and medical); the second set of questions related to the criticality of the resource to be protected (critical, essential, or required).

It should be noted that Berkeley Lab does not have any mission-critical systems as defined by DOE in its Y2K remediation guidance or its implementation of PDD 63.⁴ The survey asked, “Do you work with Mission Critical Systems at LBNL?” Although 8 of 3,473 respondents initially replied that they believed that they had mission-critical systems, follow-up by the ISSM liaisons confirmed that these identified systems were important to the Laboratory and its programs but did not meet the stated definition. Some of the respondents, however, maintain their original position. This disagreement suggests a need for Laboratory management to clarify the policy on mission-critical systems.

Similar questions regarding essential and required systems and proprietary and medical information produced a set of employees who say they are working with information or processes that may not be adequately protected by the Laboratory’s baseline measures. All of these employees can now be interviewed to determine whether their systems and information are, indeed, in need of extra protection and whether that protection is in place. By the end of this process, Berkeley Lab management will have a high degree of assurance that systems identified as needing extra protection are being protected.

CYBER SECURITY

Virus Protection. Running virus protection software is an important defense measure for Berkeley Lab considering the viruses that currently run rampant on the Internet. The questionnaire asked: “Is anti-virus software installed for all Macintosh or Windows computers you use?” The average response of 96% is excellent. This number not only

⁴ Protecting America’s Critical Infrastructures: PDD 63, May 22, 1998. This Presidential Decision Directive requires federal agencies to protect their critical physical and cyber infrastructures.

confirms that most systems are protected, but also infers that most users realize the importance of running the software. There are some systems that cannot run anti-virus software. For instance, the anti-virus was unavailable for Mac OS X until after the Self-Assessment, and some unique applications cannot work with anti-virus installed. This probably accounts for most of the 4% who do not use anti-virus.

System Vulnerabilities. Cyber security staff designed a process to uncover and correct a strictly defined and easily measurable set of high-risk computer vulnerabilities. Since vulnerabilities that appear on the network are highly dynamic, the types and duration used for this rating were fixed, limiting the actual vulnerabilities that were measured. Only those vulnerabilities that were discovered approximately eight months before the Self-Assessment were used in the Self-Assessment. While this rating does not give an indication of the current number of vulnerabilities on the Berkeley Lab networks, it does give a very accurate rating of how diligent each organization is in cleaning up known vulnerabilities.

Legal Requirements for Obtaining Software. It is important that Berkeley Lab employees do not use software illegally. This survey question represents the first step by asking if employees know what is legal. The average rating is ~85%, indicating that there is room for improved awareness of this issue, which is relatively simple and intuitive (pay for your software). It is not surprising that Facilities and EH&S rated slightly lower than the other organizations, since they rely heavily on centrally managed computer support. Many employees in these two organizations never load software and rely on their support staff to ensure Lab compliance issues.

Computer Protection Liaisons. Each Laboratory organization has a computer protection liaison whose role is to assist the Computer Protection Program Manager in the administration of the Computer Protection Program. The goal of this part of the questionnaire was to educate users that their division does, indeed, have a computer protection liaison to represent line management and assist in coordinating computer protection activities. Because a web link was provided that would answer the question, the average of 77% is somewhat disappointing. It indicates that roughly 27% not only don't know who their liaison is, but do not feel that it is worthwhile to spend a minute to find out the answer. This should be a focal point for future awareness.

Password Compliance. The purpose of this survey question is to ensure compliance with DOE password requirements.⁵ Considering that the DOE password policy is very strict and often not technically feasible, the average compliance of 91% is very good. The Computer Protection Program routinely attempts to crack Lab passwords and inform employees when their passwords need improvement. Nevertheless, Lab management will eventually have to decide if this rating is acceptable to Berkeley Lab, UC, and DOE. If not, steps will be taken to improve this rating.

Cracked Passwords. This measurement by cyber security staff is based on a defined set of ITSD-managed computers that are used by most Laboratory organizations. Security

⁵ DOE N 205.3, Password Protection, Generation, and Use, November 23, 1999.

staff do not have the technical means to collect and crack every password on every system at the Lab, so rather than measuring the actual number of bad passwords at the Lab, this measurement indicates the organization's resolve to encourage employees to use good passwords.

DOE Warning Banners. The purpose of this question is to ensure compliance with DOE warning banner requirements. While the average compliance of 87% is good, Berkeley Lab would be in a much better position to support DOE policy if compliance were closer to 100%. This year's Self-Assessment gives us a good metric of the Lab's current compliance. Warning banners were distributed to each staff member during the Self-Assessment. Next year's Self-Assessment may seek to improve this percentage. Circumstances sometimes dictate that 100% compliance with a requirement is impossible. Laboratory management will eventually have to decide what rating is acceptable to Berkeley Lab, UC, and DOE.

Backups. All important information residing on a computer should be backed up, and the result of 92% affirming that they do back up is much higher than expected and a very positive indicator.

PHYSICAL PROTECTION

Protecting Laboratory Property. In response to the question "Do you take appropriate measures to secure the property assigned to you?" the survey indicated that 98% of Lab employees make a concerted effort to secure their property. This is commendable. The small number of thefts reported at the Laboratory supports this survey result and indicates employee diligence in protecting Lab assets.

Requesting Visitor Access. A significant number of onsite staff (91%) understand how to request visitor access online. Due to heightened security awareness after 9/11, the business need to request access for visitors has driven most employees to understand this process. The results of the survey indicate a clear communication of processes to ensure visitor access. This is commendable.

Crisis Action Team. Violence in the workplace is an important issue, and Berkeley Lab has chartered and deployed the Crisis Action Team as a response to potential and actual incidents. However, the question "Are you aware of the Crisis Action Team and whom to contact regarding workplace violence?" received the lowest percentage of "yes" answers (69%) in the questionnaire. Information about the Crisis Action Team and other counseling resources should be more widely communicated by line management.

Thefts. The Site Access Office maintains a database of all reported government thefts. This database includes a summary of all reported items, dollar amounts, and a complete description of each incident. Each month, a summary is submitted to the DOE Inspector General and the LBNL Property Management Department. In addition, this data is

submitted to UC to be included in the Clery report⁶. A total of ten stolen items (\$35, 000) were reported to Site Access in 2001 (the most recent statistics available during the Self-Assessment period). In 1998, the dollar amount was \$218,000. This significant reduction is a direct result of due diligence on the part of our contracted security force as well as line management communication to identify, notify, and process all thefts.

Security Access Managers. Each Laboratory organization controls access to its own area. The people who control access are known as Security Access Managers (SAMs). Initial responses to the survey question on Security Access Managers indicate that there is confusion about the title and responsibility—half of the current SAMs checked “I am not a Security Access Manager.” Initially every Security Access Manager was provided one-on-one training, which included a packet of information, a signed contract, and posting their name on the security website. At that time, the Laboratory’s Site Access Manager explained the title, role, and responsibility for this function. Since the confusion exists, it is our recommendation that line management reinforce the role of Security Access Managers and revisit the selection of SAMs.

Card Key Access. Approximately 70% of lab employees currently utilize the card access system. As a result, a 79% survey response to the question “... do you know how to find the list of building authorizers in order to request access” is good. The purpose of the hyperlink was to educate other employees about how to request access to a card-accessed building. In the future, we may add another answer choice to capture those employees currently not affected by this process.

Keys. Because all individuals must have a key either to their building or their office, 95% of employees know about this process.

GENERAL SECURITY AWARENESS

Emergency Telephone Number. Ninety-five percent of employees know the Laboratory’s emergency telephone number. The high percentage reflects clear communication to personnel. The division with the lowest number represented employees who work offsite and use a different emergency number. In the future, the survey question will include an alternative response for offsite employees.

Employee Security Guide. During the initial rollout of the ISSM Self-Assessment, all staff received a packet of information that included a pocket-sized pamphlet, the *Employee Security Guide*. Only 89% of the employees surveyed answered that they did have access to the guide. Some employees may not have clearly understood that the distributed pamphlet was the guide. During the survey process, those who failed to acknowledge receiving a guide were encouraged to request one, and additional guides were distributed. At the conclusion of the Self-Assessment, every employee had received a pocket guide containing information and contacts for all elements of ISSM.

⁶ The “Jeanne Clery Disclosure of Campus Policy and Campus Crime Statistics Act of 1998” (20 USC §1092 (f)), commonly referred to as the Clery Act, requires institutions of higher education receiving federal financial aid to report specified crime statistics.

Improvement of the Self-Assessment Process

Experience in carrying out the first ISSM Self-Assessment and suggestions from survey participants identified several ways in which the process can be improved in the future.

SURVEY POPULATION

Who should be included in the ISSM Self-Assessment survey? Answering this question is not as easy as one might initially expect.

Faculty and visiting post-docs were excluded from the 2002 survey because they spend little time onsite, but all participating guests were initially included. RPM §1.06 provides clear definitions of participating guests: users of Laboratory User Facilities, scientific collaborators, students, nonscientific temporary or contract employees, and consultants. These guests, unlike casual visitors, should have a basic understanding of Laboratory safety and security measures.

Despite the RPM definitions, in practice the guest categories are loosely defined and may overlap with the RPM definition of casual visitor. (For example, some people who fit the RPM definition of casual visitor are given guest status so that they qualify for temporary parking permits.) Because the definitions of visitors and guests are not applied consistently, the Human Resources Information System (HRIS) database does not clearly identify who spends how much time at the lab and for what purpose. As a result, when the initial ISSM Self-Assessment survey results were tabulated and security liaisons were consulted, the ambiguity of guest status became an issue. At the recommendation of the security liaisons, some guests who spend little time onsite were eliminated from the Self-Assessment process.

Clarification of population definitions is a Lab-wide issue, as discussed below in the section “Improvement of Related Lab-Wide Processes.” Resolution of this issue will facilitate future ISSM Self-Assessments. In addition, there are other targeted groups such as construction subcontractors that might be included in some way in future Self-Assessments. The ISSM team will use the Human Resources Department’s revised definitions of *visitor* and *guest* for the next survey, including faculty and visiting post-docs.

STAFF COMMUNICATION METHODS

Secure communication with staff and guests who have LDAP usernames and passwords is easily accomplished, but communication with staff and guests without LDAP usernames is more problematic.⁷ The ISSM Self-Assessment surveyed 3,841 LDAP users and 2,170 non-LDAP users. Non-LDAP users, mostly in the Facilities and Engineering divisions, were given questionnaires on paper, and administrative staff were given

⁷ LDAP (Lightweight Directory Access Protocol) is an Internet standard database. At Berkeley Lab, LDAP is the primary database for the telephone directory, IMAP4 email, online calendar, Novell networking, employee self-service, and other functions. Everyone with an employee number is entered into LDAP, but not all employees have LDAP usernames/passwords, which would give them secure computer access to LDAP-based Laboratory services.

permission to enter their data and submit it to the ISSM Web site. Compared with the computer-only survey, the paper-plus-data-entry method increased the cost of the Self-Assessment to the Laboratory and introduced a greater potential for errors. Since LDAP is used for many other Laboratory functions besides the ISSM Self-Assessment, this issue needs to be addressed from a Lab-wide perspective, as discussed below in the section “Improvement of Related Lab-Wide Processes.” ISSM staff will require LDAP usernames and passwords for all employees and guests participating in the next Self-Assessment Survey.

QUESTIONNAIRE AND WEB SITE

Most staff found hyperlinks in the Self-Assessment survey to be a good tool to learn about security resources at the Laboratory, but the feedback indicated that some employees either failed to use the hyperlinks or did not understand their purpose. Survey instructions should clarify the function of the hyperlinks. Some participants also indicated that they want the hyperlinked information available on a Web page for future reference. Security information on the Laboratory’s Web site will be periodically reviewed and upgraded. Future questionnaires will also attempt to steer different groups into the right questions for their group, e.g., computer users/non-users, onsite/offsite employees, card key users/non-users, etc.

RAISING THE BAR

To encourage continuing improvements in security, more stringent rating criteria will be adopted in future Self-Assessments for issues such as securing assigned property, obtaining legal software, and others. For example, cyber security staff are developing a computer vulnerabilities measurement that encompasses both the existence of a vulnerability and the length of time it takes to resolve it. Although the goal of zero vulnerabilities is unattainable, this new measurement will ensure that newly discovered vulnerabilities are removed in a timely manner. Security staff are also developing methods that might broaden the scope of sampled passwords, resulting in measurements of both organization performance and the actual number of vulnerable passwords.

NEW TARGETED QUESTIONS

It is important to keep the questionnaire short to encourage a high response rate. But questions that received a high percentage of correct responses in the first Self-Assessment may be replaced by new questions that address DOE orders, audit issues, or other UC or Laboratory concerns. New topics under consideration for the next Self-Assessment include foreign visits and assignment assessments, sensitive subjects, export controls, and wireless communications. Changing the questionnaire will help the ISSM Self-Assessment promote continuing improvements in Laboratory security.

Improvement of the Laboratory’s Security Program

The Self-Assessment results identified several areas of the Laboratory’s security program that need improvement. These areas are discussed below.

ISSM WEB SITE

The ISSM Web site will be further developed to serve as a central reference for Laboratory security, with information on all the topics included in the Self-Assessment and links to other Laboratory security Web pages.

SPECIAL PROTECTION PLANS

Survey questions regarding essential and required systems and proprietary and medical information prompted some employees to say they are working with information or processes that may not be adequately protected by the Laboratory's baseline measures. All of these employees can now be interviewed to determine whether their systems and information are, indeed, in need of extra protection and whether that protection is in place. If not, special protection plans should be developed for targeted data or systems that need extra protection. ISSM staff will provide assistance and guidance.

CRISIS ACTION TEAM

Violence in the workplace is a significant issue, and Berkeley Lab has chartered and deployed the Crisis Action Team as a response to potential and actual incidents. However, the question "Are you aware of the Crisis Action Team and whom to contact regarding workplace violence?" received the lowest percentage of "yes" answers (69%) in the questionnaire. Information about the Crisis Action Team and other counseling resources should be more widely communicated by line management. Human Resources will take the lead in communicating the importance of the Crisis Action Team to line managers and supervisors.

SECURITY ACCESS MANAGERS

Each Laboratory organization controls physical access to its own area. The people who control access are known as Security Access Managers. The questionnaire results indicate that confusion still exists about the role and responsibility of Security Access Managers. Initially every Security Access Manager was provided one-on-one training, which included a packet of information, a signed contract, and posting their name on the security website. At that time, the Site Access Manager explained the role and responsibility for this function. However, since the confusion still exists, it is our recommendation that line management reinforce the role of Security Access Managers and revisit the selection of SAMs.

DATA BACKUPS

Although the 92% compliance with the requirement for data backups is much higher than expected, there is still room for improvement. Line management should ensure that important information is appropriately backed up. ISSM staff will provide guidance on appropriate data backup systems.

LEGAL REQUIREMENTS FOR OBTAINING SOFTWARE

The average rating of 85% on this question indicates that there is room for improved awareness of this issue. Line management should reinforce the policy on legal requirements for obtaining software.

COMPUTER PROTECTION LIAISONS

The survey indicates that roughly 27% of staff not only do not know who their liaison is, but do not feel that it is worthwhile to spend a minute to find out the answer. We recommend that line management remind staff of who their computer protection liaisons are and what services they provide.

PASSWORD COMPLIANCE

Considering that the DOE password policy is very strict and often not technically feasible, the average compliance of 91% is very good. Nevertheless, Laboratory management will have to decide if this rating is acceptable to Berkeley Lab, UC, and DOE on the basis of a cost/benefit/security analysis. ISSM staff will conduct this analysis.

DOE WARNING BANNERS

While the average compliance of 87% is good, Berkeley Lab would be in a much better position to support DOE policy if compliance were closer to 100%. Next year's Self-Assessment may seek to improve this percentage. Lab management will have to come to a conclusion on what rating is acceptable to Berkeley Lab, UC, and DOE on the basis of a cost/benefit/security analysis. ISSM staff will conduct this analysis.

Improvement of Related Lab-Wide Processes

The Self-Assessment process identified several related Lab-wide processes that need improvement. These issues are discussed below.

POPULATION DEFINITIONS

As described above, the RPM definitions of *visitor* and *participating guest* are not applied consistently, and the definition of guests does not clearly specify how much time the guest spends at the Laboratory. As a result, these categories are inadequate not just for determining the appropriate population for the ISSM Self-Assessment survey, but also for various reporting requirements, such as the new DOE Foreign Visit and Assignment identification and the annual vehicle and personnel count for the City of Berkeley.

The DOE defines a *visitor* as someone who is onsite for less than 30 days in a calendar year, while an *assignee* is onsite for 30 or more days. We recommend that Human Resources consider redefining the *visitor* and *guest* categories in a way that is consistent with DOE guidance and that clearly specifies the amount of time spent onsite for all categories. Such a redefinition would facilitate various reporting requirements as well as the ISSM Self-Assessment survey and other security functions. Human Resources is taking this under consideration and formulating a recommendation.

STAFF COMMUNICATION METHODS

As discussed above, secure communication with staff and guests who have LDAP usernames is easily accomplished, but communication with staff and guests without LDAP usernames is more expensive and, in cases like the Self-Assessment survey, more susceptible to error. Some staff do not have LDAP usernames because they do not use a computer in their everyday work; some may use computer systems that are not compatible with LDAP; and some may simply choose not to have an LDAP username.

An inexpensive shared computer in each work unit would make LDAP access easily available to all employees and guests, and most employees already enter their time on their own or a shared computer. Considering how many Laboratory functions depend on LDAP—directory, calendar, email, Human Resources data, vehicle data, and others—we recommend that Laboratory management adopt LDAP usernames and passwords as the Lab standard for authentication and access to institutional resources for all employees and guests. Other access methods should not be supported. ISSM staff will require LDAP usernames and passwords for all employees and guests participating in the next Self-Assessment Survey.

MISSION-CRITICAL SYSTEMS

The survey revealed some confusion about LBNL definitions of mission-critical, essential, and required systems. These definitions should be revisited and a clear policy on the operation of mission-critical systems should be adopted and communicated to staff. ISSM staff will recommend criteria for the definition of mission-critical systems.

Action Items

Line Management

1. Adopt LDAP usernames and passwords as the Lab standard for authentication and access to institutional resources for all employees and guests. Other access methods will not be supported. Ensure that all employees and guests have LDAP usernames and access to a networked computer.
2. Redefine the *visitor* and *guest* categories in a way that is consistent with DOE guidance and that clearly specifies the amount of time spent onsite for all categories. The Human Resources Department will take the lead on this item and will communicate the new definitions to Lab personnel.
3. Revisit the definition of mission-critical systems and adopt and communicate a clear policy on the operation of mission-critical systems to staff. ISSM staff will assist in formulating the definition.
4. Develop special protection plans for targeted data or systems that need extra protection, if that protection is not already in place. ISSM staff will provide assistance and guidance.
5. Communicate information about the purpose and function of the Crisis Action Team. Human Resources will provide this information to line managers.

6. Reinforce the role of Security Access Managers and revisit the selection of SAMs.
7. Remind staff of who their computer protection liaisons are and what services they provide.
8. Ensure that important information is appropriately backed up. ISSM staff will provide guidance on appropriate data backup systems.
9. Reinforce the policy on legal requirements for obtaining software.

ISSM Staff

1. Require LDAP usernames and passwords for all employees and guests participating in the next Self-Assessment Survey.
2. Recommend criteria for the definition of mission-critical systems.
3. Provide assistance and guidance for developing special protection plans.
4. Recommend criteria for backups.
5. Develop the ISSM Web site to serve as a central reference for Laboratory security, with information on all the topics included in the Self-Assessment and links to other Laboratory security Web pages.
6. Assess whether the password compliance rating is acceptable to Berkeley Lab, UC, and DOE on the basis of a cost/benefit/security analysis.
7. Assess whether the DOE warning banner rating is acceptable to Berkeley Lab, UC, and DOE on the basis of a cost/benefit/security analysis.

Appendix A

Integrated Safeguards and Security Management Plan



Integrated Safeguards and Security Management Plan (ISSM) for the Ernest Orlando Lawrence Berkeley National Laboratory

Contents

[Vision Statement](#)

[Mission Statement](#)

[Introduction](#)

[Guiding Security Principles](#)

[External Controls](#)

[Security Functions at the Institutional Level](#)

[Security Functions at the Division, Project or Activity Level](#)

[Security Management Plan Summary](#)

[2002 ISSM Self-Assessment Results](#)

Final

Effective Date: April 16, 2001

**Environment, Health and Safety Division
Lawrence Berkeley National Laboratory
University of California
Berkeley, CA 94720**

Prepared for the U.S. Department of Energy under
Contract Number DE-AC03-76SF00098

Approved By:

Charles V. Shank
Director
Lawrence Berkeley National Laboratory

Richard H. Nolan
Director & Site Manager
DOE Berkeley Site Office

Approved By:

Functional Managers

A.X Merola
Division Director
Information Technologies and Services Division

Donald W. Bell
Property Protection, Life Safety Manager
Environment, Health and Safety Division

Cheryl A. Fragiadakis
Technology Transfer Department Head
Technology Transfer Department

David J. Aston
Export Control Officer
Directorate

Guy Bear
(Acting) Human Resources Head
Human Resources Department

The following informative Appendices do not appear in this document. For information concerning this material, see the web sites provided.

[Appendix A. Safeguards and Security Plan](#)

[Appendix B. Cyber Security Protection Plan](#)

[Appendix C. Export Control Document](#)

[Appendix D. Counter Intelligence Plan](#)

Appendix E. Security Reference Guide (Future Site)

A. Vision Statement

Integrated security supports and protects innovative science.

B. Mission Statement

The Berkeley Lab Security program assures all visitors and employees of an open and secure work environment that fosters the continuation of creative scientific advances. Integrated security management ensures the protection of Laboratory assets, including physical and intellectual property, and establishes programs for cyber security, export control and counterintelligence.

C. Introduction

Ernest Orlando Lawrence Berkeley National Laboratory (Berkeley Lab) is a multidisciplinary national research laboratory, located on land belonging to the Regents of the University of California and operated with funds furnished by the U.S. Department of Energy (DOE). As stewards of this public trust, the staff and management of Berkeley Lab must protect the public's interest and investment in the people, the land and environment, the equipment and facilities and the intellectual property that make up Berkeley Lab.

Berkeley Lab sets policy to ensure a secure working environment for all employees and visitors. As a designated Tier Three laboratory managed by the University of California and under contract to DOE, all practices established must ensure an open, collaborative work environment that facilitates scientific excellence. The Laboratory must achieve a balance between protecting its critical assets and maintaining this open working environment that supports collaborative science. Since the Laboratory is engaged in an unclassified mission, the security threats are deemed to be relatively low compared to other DOE sites in the Tier I and II categories.

The Laboratory's mission includes not only fundamental science in partnership with research universities and other national laboratories, but also collaborative research in participation with industry and the world scientific community. Research is reviewed for export controls designed to protect items and information determined to be important to the national interest.

D. Guiding Security Principles

High standards of performance and clearly defined expectations result in a safe and secure working environment. In its commitment to scientific excellence, Berkeley Lab adheres to the following guiding security principles:

- *Line management owns security.* Every laboratory manager is responsible for integrating appropriate security controls into his/her work and for ensuring active communications of security expectations up and down the management line and with the workforce.
- *Clear roles and responsibilities are defined and communicated.* Clear lines of authority and responsibility for security assurances are established and met. At Berkeley Lab this principle is manifested in position descriptions, and performance reviews, as well as feedback up and down the line.

- *Cyber and physical security, export control management, and counterintelligence functions are integrated.* All employees are provided with the necessary resources to identify the functions that affect their work environment. They not only have the information required, but also understand their individual responsibility to guard and protect these assets.
- *An open environment supports the Berkeley Lab mission.* As a Tier Three Laboratory, it is vital that collaborative research be conducted with Tier One and Tier Two laboratories, as well as with industry, universities, and the international scientific community. The Laboratory must be open and accessible.
- *Security is a value-added activity supporting research and support operations.* Security must support the Laboratory's mission.
- *Security controls are tailored to individual and facility requirements.* Each division will designate a security point of contact. This contact will work directly with the Environment, Health & Safety (EH&S) and Computing Sciences (CS) security managers to lay out an integrated security plan to meet the business needs of the group. The point of contact will develop both individual and group approaches for Laboratory security requirements. Not every aspect of security requirements, such as counter intelligence issues or export control requirements, will affect every individual or group. However, every group should be able to identify when these requirements affect their work.

While these security principles apply to all work performed at Berkeley Lab, the implementation of these principles continues to be flexible as we maintain an open, collaborative work environment while at the same time identifying and mitigating any threats. Therefore, policy, performance, and review standards should be commensurate with those for a low-risk, unclassified laboratory. Clear communication between all Laboratory visitors and employees is an essential ingredient to maintain this climate while protecting our assets. Principal investigators (PI)s, managers and supervisors are expected to incorporate these principles into the management of their work activities. Not only does the Laboratory maintain an open facility on site, but we also manage facilities on campus at UC Berkeley, as well as downtown Berkeley, Oakland and Walnut Creek. These on-site and off-site facilities follow the same program principle.

Figure A illustrates the relationship that must exist between the external organization, the Laboratory, the division and line management to protect Berkeley Lab's assets and provide the necessary controls.

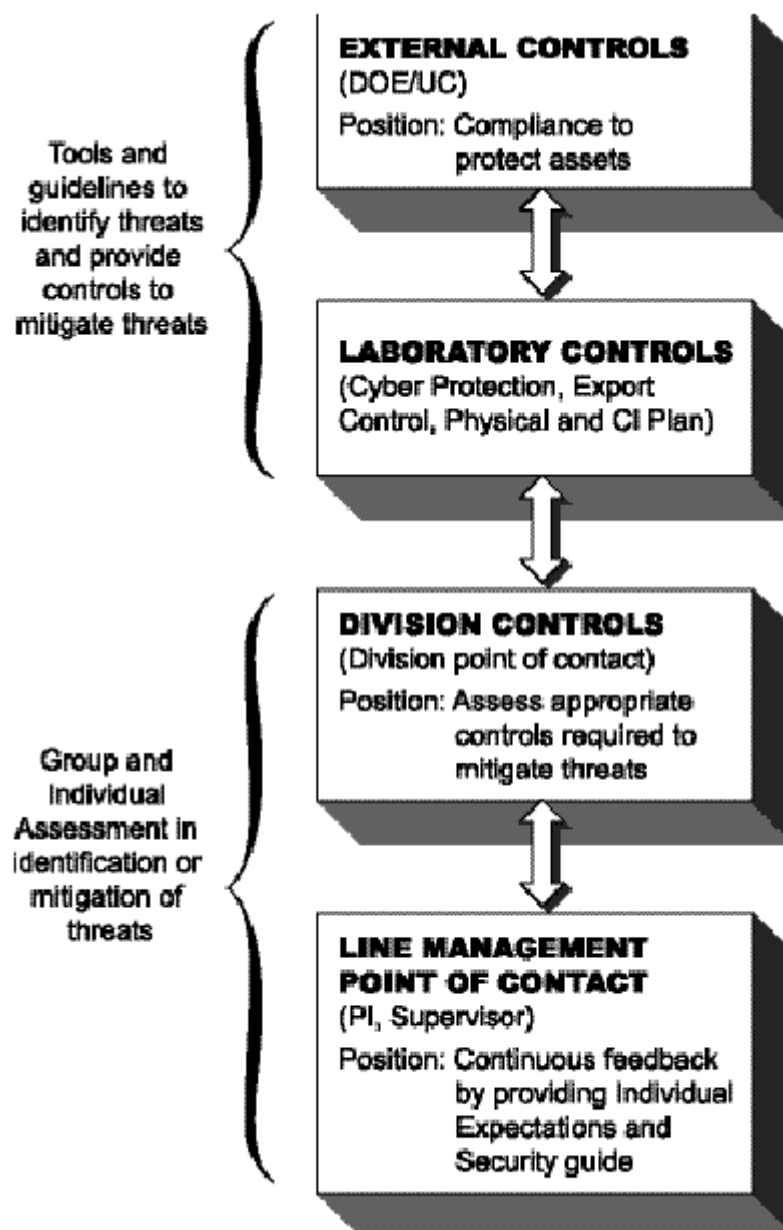


Figure A. Integrated Controls.

E. External Controls

The Laboratory's principal role for DOE is fundamental science. Our multidisciplinary research environment and unique location serve to strengthen partnerships with industry, universities and other government laboratories. These roles support DOE's Strategic Laboratory Missions Plan and are based on core competencies. How to maintain an open collaborative environment and still protect its assets will require that the Laboratory engage in an ongoing dialogue with its stakeholders. As we attempt to achieve the proper balance between collaboration and security, this Security Management Plan will provide the tools for analysis and feedback. External and internal institutional assessment will govern the future direction of the plan. Ongoing feedback will be the relevant tool to ensure that science is not encumbered and that the necessary resources are provided without jeopardizing our security principles.

Some of the organizations with the more significant roles include:

- DOE – Office of Security Operations (SO)
- DOE – Office of Science (SC)
- DOE – BSO
- University of California President's Council on Security
- University of California Office of the President
- Computer Incident Advisory Council (CIAC)

Security policy is initiated at the institutional level and from DOE headquarters. As indicated in Section II of the Institutional Plan, the Laboratory implements physical security programs appropriate for the protection of its employees and Lab property. The adequacy of Berkeley Lab's security management systems is reviewed periodically by senior management. Mechanisms for conducting this review include independent peer reviews.

F. Security Functions at the Institutional Level

It is the responsibility of Computing Sciences and the Property Protection, Life Safety Group (PPLS) in the EH&S Division to provide guidance to each Berkeley Lab division in assessing and mitigating security threats. Security threats for LBNL are found in Appendices A and B. This procedure guarantees high quality standards and clearly defined expectations that will result in a safe, secure working environment for every employee and visitor. Based on guidance provided by the managers of the cyber and physical security programs, divisions may identify the threats applicable to their work. Working in coordination with the institutional program managers, divisions must institute controls commensurate with the threat. The following items are examples of security functions at the institutional level.

1. *Work planning.* The tasks to be accomplished as part of any given activity are defined clearly. As stated in the Laboratory Institutional Plan, programmatic goals are managed through divisions that implement DOE and other sponsors' research programs. These divisions have line and project management responsibility to assure that intellectual, property, computa

and other resources are properly protected to sustain the scientific mission and operational requirements. Security planning is integrated with scientific and operations planning.

2. *Analyze threats to the extent possible.* Security vulnerabilities associated with performing planned work are clearly identified and understood before beginning work. Threats to Berkeley Lab work are stated in the Cyber and Physical Security Plans.
3. *Develop appropriate countermeasures to threats, and communicate information regarding threats, countermeasures and controls.* Appropriate counter measures are in place. These measures are based on best standards and are reviewed periodically. All visitors and employees receive the required information regarding threats and methods for mitigating threats.

The following documents provide the necessary controls adopted at the Laboratory:

- Safeguards and Security Plan
- Cyber Security Protection Program
- Export Control Document
- Counter Intelligence Plan

Since all work at the Laboratory is carried out under contract with the Regents of the University of California and the U.S. Department of Energy, fundamental controls are developed and agreed upon by the Laboratory.

4. *Perform work within the controls.* Once controls are identified, line management must ensure that work is executed within those controls.
5. *Continuous feedback.* Security measures are continually assessed for effectiveness through operational awareness. In addition, periodic reviews, such as external peer reviews, are conducted.

G. Security Functions at the Division, Project or Activity Level

In order to provide an appropriate level of security and meet DOE and statutory requirements, Berkeley Lab requires commitment and leadership from management in communicating to our visitors and employees our value-added security program. It is the responsibility of Computing Sciences and the Property Protection, Life Safety Group (PPLS) in the EH&S Division to provide guidance to each division in assessing and mitigating security threats. This process guarantees high standards and clearly defined controls that will result in a secure working environment for every employee and visitor.

The Laboratory has established a unified set of security elements to protect critical assets. A Security Reference Guide will be provided to all Laboratory employees and visitors. External peer reviews and internal reviews afford the essential feedback to ensure that all security controls are in place. The critical assets of personnel, physical and information security are continually evaluated.

Figure B illustrates the correlation that exists in protecting the critical assets of the Laboratory and the documentation and review process necessary for continual feedback.

Berkeley Lab's research and support divisions vary widely in the type of work performed, size, location and customers. Accordingly, each division's threats and assets are different. While following broad Laboratory security policy, it is appropriate for each division, with assistance from the

institution, to tailor its security programs to its needs.

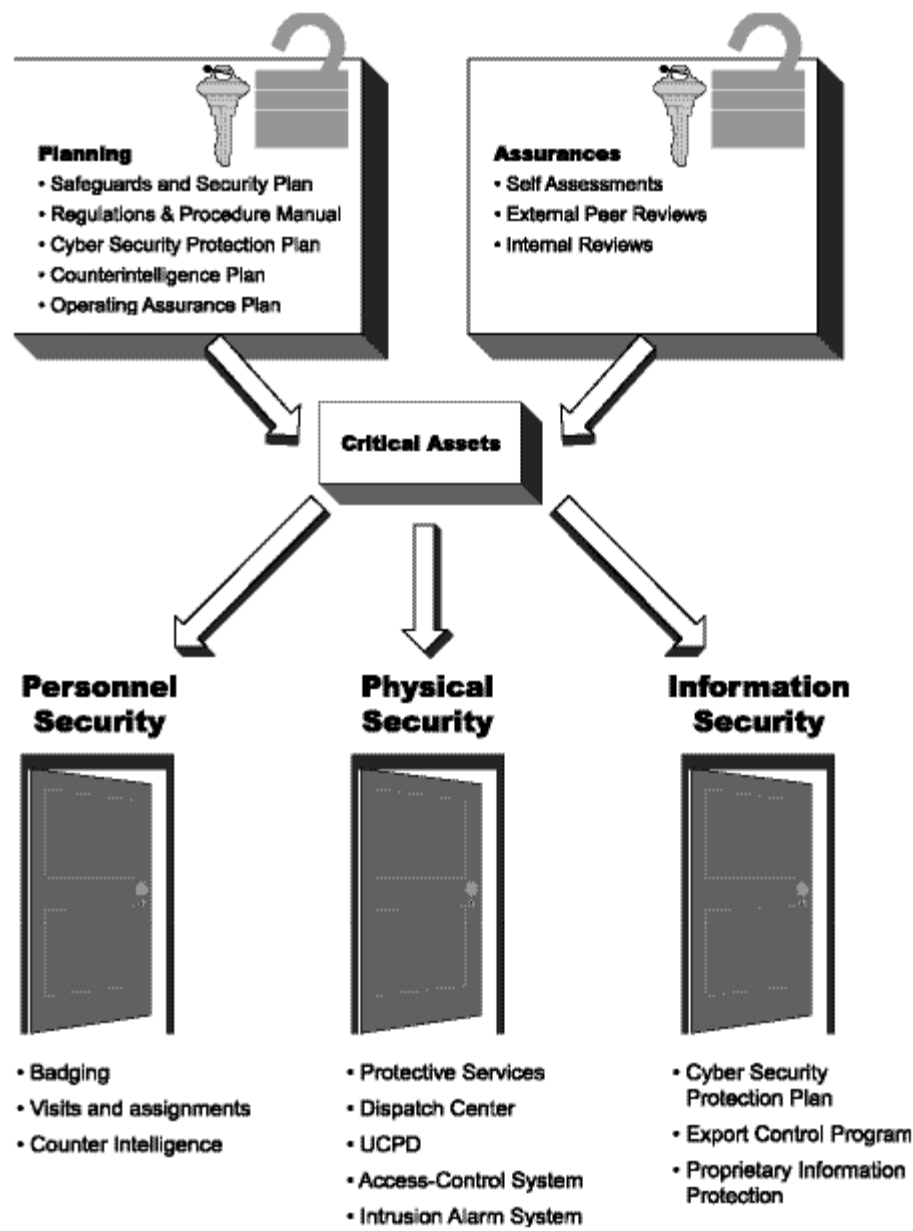


Figure R. Berkeley Lab employs integrated security elements to protect critical assets.

1. *Work planning.* At the beginning of any new initiative or building construction, the division in partnership with the Cyber and Physical Security managers will define the work and function within that environment. Consideration will be given to cost and building location, and ensure that all credible threats have been identified and all preventive measures implemented.
2. *Define the required security elements and threats.* As part of the planning process, PIs, managers and supervisors are required to consider what threats are present and to implement

- appropriate controls as outlined in the Security Reference Guide. They are required to assure that every employee is in conformance with security requirements. For the majority of the work, threats are minimal and security precautions are routine.
3. *Develop appropriate countermeasures to threats, and communicate information regarding threats, countermeasures and controls.* Appropriate controls for activities at Berkeley Lab are described in the Site Safeguards and Security Plan. Four countermeasure strategies used include access denial, access control, intrusion warning, and intervention. The degree to which these strategies are employed depends on the level of risk the threat presents.
 4. *Perform work within those controls.* Use security tools, guidelines and resources to ensure the work is performed within the established controls. A printed security guide will be distributed to every employee; the guide will contain information about security threats, methods for mitigation, and resources or points of contact. Expectations for each employee will be clearly stated in the yearly appraisal process.
 5. *Continuous feedback.* All security measures are assessed on an ongoing basis through operational awareness. In addition, periodic reviews, such as external peer reviews, are conducted.

Figure C clarifies the roles and responsibilities of an integrated security management plan. The relationship between senior management, the division and line management requires continuous feedback to ensure that all work performed meets all security criteria.

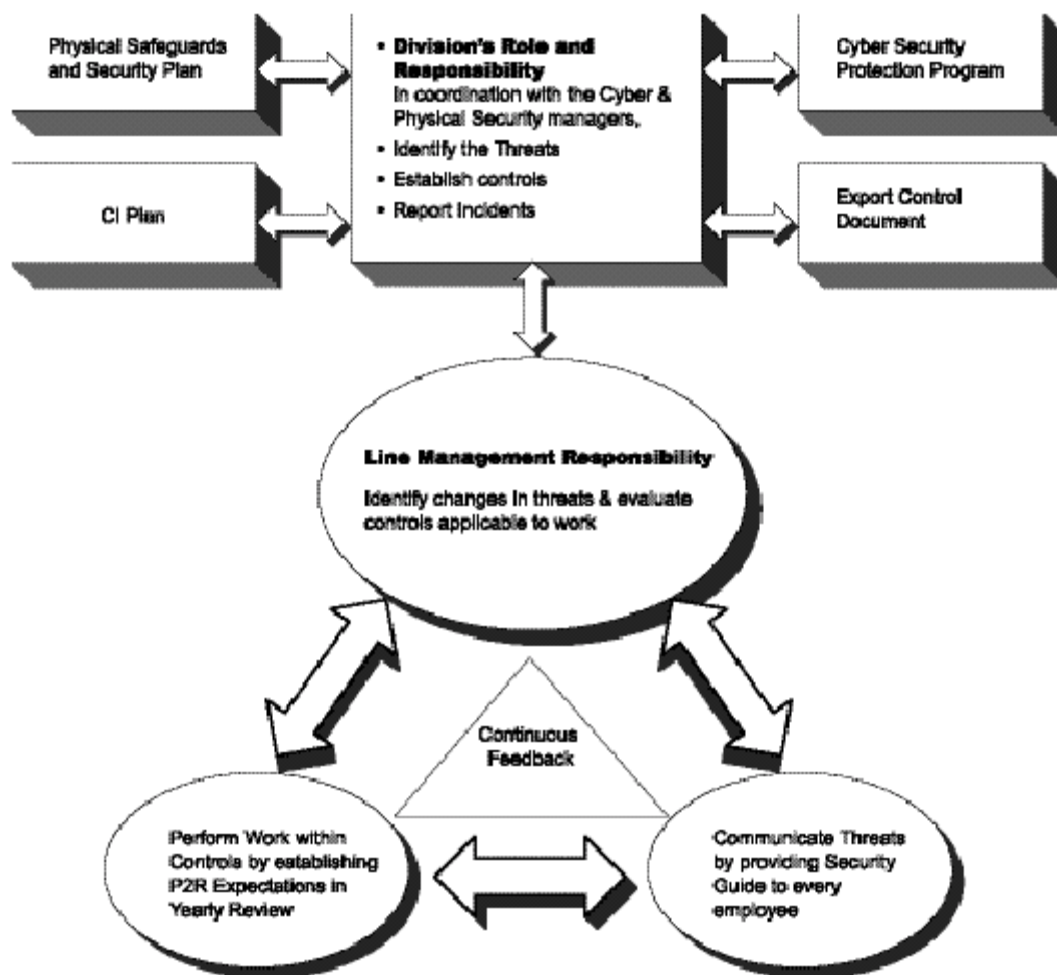


Figure C. Roles and responsibilities of an Integrated Security Management Plan.

H. Security Management Plan Summary

Berkeley Lab is committed to scientific excellence and stewardship of its assets. While security principles apply to all work performed at the Laboratory, their implementation is flexible. Berkeley Lab adheres to the following principles:

- Line management owns security.
- Security roles and responsibilities are clearly defined and communicated.
- Security functions are integrated.
- An open environment supports the Laboratory's Mission.
- The security program must support the scientific and operational missions of the Laboratory and must be value added.
- Security controls are tailored to individual and facility requirements.

[Top](#) | [Physical Security & Property Protection](#) | [ISSM Home](#)

Appendix B

Self-Assessment Questionnaire

Integrated Safeguards and Security Management

Please ensure that an appropriate response is given for each question.

ISSM DIVISION SELF-ASSESSMENT QUESTIONNAIRE

Employee/Guest Name: _____

Date: _____

Employee/Guest ID Num: _____

Division: _____

Q1. Do you know the [emergency phone number for the Laboratory](#)?

☐ Yes

☐ No

Q2. Do you have access to the [Employee Security Guide](#)?

☐ Yes

☐ No

Q3. Do you currently hold a [security clearance](#) that allows access to classified information? You should know if you hold a security clearance. If you are uncertain, it is unlikely that you have one.

☐ Yes

☐ No

Q4. If a building has the new proximity card access system, do you know how to find the [list of building authorizers](#) in order to request access?

☐ Yes

☐ No

Q5. Do you know how to [request access for your visitors](#)?

☐ Yes

☐ No

Q6. Do you know [whom to contact](#) regarding keys to your office or building?

☐ Yes

☐ No

Q7. Do you take appropriate measures to [secure the property](#) assigned to you?

☐ Yes

☐ No

- Q8. If you are a [Security Access Manager](#), do you review your access lists annually?
- ☐ I am not a Security Access Manager
 - ☐ Yes
 - ☐ No
- Q9. Are you aware of the [Crisis Action Team](#) and whom to contact regarding [workplace violence](#)
- ☐ Yes
 - ☐ No
- Q10. Do you know the Lab's [legal requirements](#) for obtaining software?
- ☐ Yes
 - ☐ No
 - ☐ I do not use a computer at work
- Q11. Do you have a [warning banner](#) on all computers you are responsible for?
- ☐ Yes
 - ☐ No
 - ☐ I do not use a computer at work
- Q12. Do you change your password according to the LBNL [password policy](#)?
- ☐ Yes
 - ☐ No
 - ☐ I do not use a computer at work
- Q13. Is [anti-virus software](#) installed for all Macintosh or Windows computers you use?
- ☐ Yes
 - ☐ No
 - ☐ I do not use a computer at work
- Q14. Do you know who your [Computer Protection Liaison](#) is?
- ☐ Yes
 - ☐ No
 - ☐ I do not use a computer at work
- Q15. Do you [back up](#) all information that you deem important to your work?
- ☐ Yes
 - ☐ No

☐ I do not use a computer at work

Q16. Do you work with the following types of information at LBNL:

[Classified Information](#)

☐ Yes

☐ No

[Unclassified Controlled Nuclear Information \(UCNI\)](#)

☐ Yes

☐ No

[Naval Nuclear Propulsion \(NNPI\)](#)

☐ Yes

☐ No

[Proprietary Information](#)

☐ Yes

☐ No

[Personal Medical Information](#)

☐ Yes

☐ No

Q17. Do you have any information or processes that may result in significant injury or damage (millions of dollars) if the information or process becomes unavailable for:

up to 10 seconds ([Mission Critical](#))

☐ Yes

☐ No

up to 24 hours ([Essential System](#))

☐ Yes

☐ No

up to 5 days ([Required System](#))

☐ Yes

☐ No

Q18. Additional comments or suggestions:

Appendix C

Detailed Survey Results

This appendix contains detailed results for questions that were rated in the organizational and institutional profiles. Non-rated statistical questions are not included here, but are reported in the organizational profiles, Appendix E.

Survey Completion Summary

	10-29			2-19			
		0 - 50 Red	50 - 70 Yellow	70 -100 Green			
DIV	Total	Complete	Pct		Total	Complete	Pct
AD	332	316	95.18%		330	317	96.06%
AF	130	123	94.62%		127	123	96.85%
AL	203	171	84.24%		203	172	84.73%
CF	80	77	96.25%		80	77	96.25%
CH	96	57	59.38%		96	58	60.42%
CS	31	21	67.74%		31	22	70.97%
EE	310	215	69.35%		308	215	69.81%
EG	427	407	95.32%		421	418	99.29%
EH	146	141	96.58%		146	142	97.26%
ES	198	164	82.83%		186	184	98.92%
FA	339	321	94.69%		337	324	96.14%
GN	138	132	95.65%		139	135	97.12%
HR	76	72	94.74%		76	75	98.68%
IC	226	190	84.07%		227	205	90.31%
LD	70	62	88.57%		69	67	97.10%
LS	350	283	80.86%		349	283	81.09%
MS	297	226	76.09%		259	223	86.10%
NE	189	156	82.54%		188	158	84.04%
NS	134	117	87.31%		134	128	95.52%
OP	17	14	82.35%		18	15	83.33%
PB	136	79	58.09%		135	97	71.85%
PH	175	129	73.71%		163	142	87.12%
Total	4100	3473	84.71%		4022	3580	89.01%

Question 1: Do you know the emergency phone number for the Laboratory?

Answer: <http://isswdev/ISSM/definitions/EmpSecGuide.html#LabEmergencyPhone>

	10-29			<i>0 - 60 Red</i>	<i>60 - 85 Yellow</i>	<i>85 - 100 Green</i>	2-19		
DIV	Total	Yes	Pct				Total	Yes	Pct
AD	315	297	94.29%				317	304	95.90%
AF	124	119	95.97%				123	119	96.75%
AL	174	165	94.83%				172	163	94.77%
CF	77	73	94.81%				77	75	97.40%
CH	59	55	93.22%				58	54	93.10%
CS	21	21	100.00%				22	22	100.00%
EE	214	200	93.46%				215	200	93.02%
EG	409	393	96.09%				418	413	98.80%
EH	136	133	97.79%				142	140	98.59%
ES	163	157	96.32%				184	179	97.28%
FA	331	317	95.77%				324	311	95.99%
GN	132	117	88.64%				135	127	94.07%
HR	72	69	95.83%				75	74	98.67%
IC	190	184	96.84%				205	199	97.07%
LD	62	58	93.55%				67	62	92.54%
LS	280	268	95.71%				283	271	95.76%
MS	225	212	94.22%				222	209	94.14%
NE	154	150	97.40%				158	154	97.47%
NS	115	109	94.78%				128	121	94.53%
OP	14	14	100.00%				15	15	100.00%
PB	78	74	94.87%				97	92	94.85%
PH	128	118	92.19%				142	130	91.55%
Total	3473	3303	95.11%				3579	3434	95.95%

Question 2: Do you have access to the Employee Security Guide?

Answer: <http://isswdev/ISSM/definitions/EmpSecGuide.html>

	10-29			<i>0 - 60 Red</i>	<i>60 - 85 Yellow</i>	<i>85 - 100 Green</i>	2-19		
DIV	Total	Yes	Pct				Total	Yes	Pct
AD	315	286	90.79%				317	291	91.80%
AF	124	112	90.32%				123	112	91.06%
AL	174	147	84.48%				172	145	84.30%
CF	77	60	77.92%				77	74	96.10%
CH	59	55	93.22%				58	55	94.83%
CS	21	21	100.00%				22	22	100.00%
EE	214	193	90.19%				215	194	90.23%
EG	409	358	87.53%				418	372	89.00%
EH	136	121	88.97%				142	131	92.25%
ES	163	137	84.05%				184	169	91.85%
FA	331	263	79.46%				324	268	82.72%
GN	132	118	89.39%				135	127	94.07%
HR	72	68	94.44%				75	72	96.00%
IC	190	176	92.63%				205	191	93.17%
LD	62	58	93.55%				67	63	94.03%
LS	280	260	92.86%				283	263	92.93%
MS	225	201	89.33%				222	200	90.09%
NE	154	142	92.21%				158	146	92.41%
NS	115	95	82.61%				128	116	90.63%
OP	14	14	100.00%				15	15	100.00%
PB	78	67	85.90%				97	83	85.57%
PH	128	114	89.06%				142	127	89.44%
Total	3473	3066	88.28%				3579	3236	90.42%

Question 4: If a building has the new proximity card access system, do you know how to find the list of building authorizers in order to request access?

Answer: <http://www.lbl.gov/Workplace/site-access/access/SAM.html>

	10-29			<i>0 - 50 Red</i>	<i>50 - 70 Yellow</i>	<i>70 - 100 Green</i>	2-19		
DIV	Total	Yes	Pct				Total	Yes	Pct
AD	315	257	81.59%				317	265	83.60%
AF	124	86	69.35%				123	86	69.92%
AL	174	146	83.91%				172	144	83.72%
CF	77	51	66.23%				77	53	68.83%
CH	59	49	83.05%				58	49	84.48%
CS	21	19	90.48%				22	20	90.91%
EE	214	175	81.78%				215	175	81.40%
EG	409	298	72.86%				418	308	73.68%
EH	136	104	76.47%				142	117	82.39%
ES	163	131	80.37%				184	151	82.07%
FA	331	242	73.11%				324	237	73.15%
GN	132	96	72.73%				135	112	82.96%
HR	72	60	83.33%				75	62	82.67%
IC	190	163	85.79%				205	175	85.37%
LD	62	49	79.03%				67	53	79.10%
LS	280	248	88.57%				283	251	88.69%
MS	225	185	82.22%				222	183	82.43%
NE	154	131	85.06%				158	134	84.81%
NS	115	95	82.61%				128	109	85.16%
OP	14	11	78.57%				15	13	86.67%
PB	78	64	82.05%				97	78	80.41%
PH	128	83	64.84%				142	92	64.79%
Total	3473	2743	78.98%				3579	2867	80.11%

Question 5: Do you know how to request access for your visitors?

Answer: http://ia-webserver.lbl.gov:591/visitor_pass/

	10-29			<i>0 - 60 Red</i>	<i>60 - 85 Yellow</i>	<i>85 - 100 Green</i>	2-19		
DIV	Total	Yes	Pct				Total	Yes	Pct
AD	315	307	97.46%				317	310	97.79%
AF	124	113	91.13%				123	113	91.87%
AL	174	161	92.53%				172	159	92.44%
CF	77	60	77.92%				77	61	79.22%
CH	59	53	89.83%				58	52	89.66%
CS	21	19	90.48%				22	21	95.45%
EE	214	205	95.79%				215	206	95.81%
EG	409	359	87.78%				418	372	89.00%
EH	136	121	88.97%				142	131	92.25%
ES	163	152	93.25%				184	175	95.11%
FA	331	272	82.18%				324	266	82.10%
GN	132	116	87.88%				135	127	94.07%
HR	72	70	97.22%				75	74	98.67%
IC	190	180	94.74%				205	194	94.63%
LD	62	58	93.55%				67	62	92.54%
LS	280	272	97.14%				283	275	97.17%
MS	225	205	91.11%				222	204	91.89%
NE	154	143	92.86%				158	147	93.04%
NS	115	105	91.30%				128	115	89.84%
OP	14	13	92.86%				15	14	93.33%
PB	78	72	92.31%				97	89	91.75%
PH	128	114	89.06%				142	127	89.44%
Total	3473	3170	91.28%				3579	3294	92.04%

Question 6: Do you know whom to contact regarding keys to your office or building?

Answer: <http://www.lbl.gov/Workplace/site-access/access/bldgAccess.html#keys>

	10-29			<i>0 - 50 Red</i>	<i>50 - 70 Yellow</i>	<i>70 - 100 Green</i>	2-19		
DIV	Total	Yes	Pct				Total	Yes	Pct
AD	315	303	96.19%				317	306	96.53%
AF	124	120	96.77%				123	119	96.75%
AL	174	164	94.25%				172	162	94.19%
CF	77	73	94.81%				77	75	97.40%
CH	59	54	91.53%				58	53	91.38%
CS	21	18	85.71%				22	19	86.36%
EE	214	197	92.06%				215	197	91.63%
EG	409	378	92.42%				418	393	94.02%
EH	136	127	93.38%				142	134	94.37%
ES	163	155	95.09%				184	174	94.57%
FA	331	313	94.56%				324	308	95.06%
GN	132	126	95.45%				135	132	97.78%
HR	72	69	95.83%				75	73	97.33%
IC	190	184	96.84%				205	197	96.10%
LD	62	54	87.10%				67	59	88.06%
LS	280	275	98.21%				283	278	98.23%
MS	225	218	96.89%				222	215	96.85%
NE	154	147	95.45%				158	151	95.57%
NS	115	110	95.65%				128	122	95.31%
OP	14	14	100.00%				15	15	100.00%
PB	78	75	96.15%				97	94	96.91%
PH	128	121	94.53%				142	135	95.07%
Total	3473	3295	94.87%				3579	3411	95.31%

Question 7: Do you take appropriate measures to secure the property assigned to you?

Answer: <http://www.lbl.gov/Workplace/Property-Services/propguide/propertyguide.html#propertyCustodians>

	10-29			<i>0 - 60 Red</i>	<i>60 - 85 Yellow</i>	<i>85 - 100 Green</i>	2-19		
DIV	Total	Yes	Pct				Total	Yes	Pct
AD	315	310	98.41%				317	312	98.42%
AF	124	122	98.39%				123	121	98.37%
AL	174	174	100.00%				172	172	100.00%
CF	77	74	96.10%				77	74	96.10%
CH	59	56	94.92%				58	55	94.83%
CS	21	20	95.24%				22	22	100.00%
EE	214	208	97.20%				215	209	97.21%
EG	409	397	97.07%				418	418	100.00%
EH	136	136	100.00%				142	142	100.00%
ES	163	160	98.16%				184	180	97.83%
FA	331	322	97.28%				324	315	97.22%
GN	132	131	99.24%				135	134	99.26%
HR	72	70	97.22%				75	73	97.33%
IC	190	188	98.95%				205	203	99.02%
LD	62	62	100.00%				67	66	98.51%
LS	280	273	97.50%				283	276	97.53%
MS	225	221	98.22%				222	219	98.65%
NE	154	153	99.35%				158	157	99.37%
NS	115	112	97.39%				128	124	96.88%
OP	14	14	100.00%				15	15	100.00%
PB	78	78	100.00%				97	95	97.94%
PH	128	126	98.44%				142	139	97.89%
Total	3473	3407	98.10%				3579	3521	98.38%

Question 8: If you are a Security Access Manager, do you review your access lists annually?

2-19-03

DIV	EMPID	Name	"Wrong" response
FA	230251	McPherson, David L	No
FA	281851	Trigales, Kevin P	No
FA	194201	Wu, William H	No

Question 9: Are you aware of the Crisis Action Team and whom to contact regarding workplace violence

Answer: <http://www.lbl.gov/LBL-Work/RPM/R2.05.html#RTFToC27>

	10-29			<i>0 - 50 Red</i>	<i>50 - 70 Yellow</i>	<i>70 - 100 Green</i>	2-19		
DIV	Total	Yes	Pct				Total	Yes	Pct
AD	315	203	64.44%				317	252	79.50%
AF	124	82	66.13%				123	82	66.67%
AL	174	142	81.61%				172	140	81.40%
CF	77	42	54.55%				77	45	58.44%
CH	59	42	71.19%				58	43	74.14%
CS	21	16	76.19%				22	17	77.27%
EE	214	144	67.29%				215	144	66.98%
EG	409	258	63.08%				418	265	63.40%
EH	136	97	71.32%				142	109	76.76%
ES	163	108	66.26%				184	150	81.52%
FA	331	201	60.73%				324	211	65.12%
GN	132	93	70.45%				135	110	81.48%
HR	72	50	69.44%				75	56	74.67%
IC	190	144	75.79%				205	152	74.15%
LD	62	41	66.13%				67	45	67.16%
LS	280	220	78.57%				283	223	78.80%
MS	225	161	71.56%				222	160	72.07%
NE	154	113	73.38%				158	117	74.05%
NS	115	70	60.87%				128	102	79.69%
OP	14	12	85.71%				15	13	86.67%
PB	78	55	70.51%				97	71	73.20%
PH	128	72	56.25%				142	80	56.34%
Total	3473	2366	68.13%				3579	2587	72.28%

Question 10: Do you know the Lab's legal requirements for obtaining software?

Answer: <http://www.lbl.gov/ITSD/CIS/Software/licensing.html>

	10-29				0 - 60 Red				60 - 85 Yellow				85 - 100 Green				2-19			
DIV	DontUs	Yes	No	Pct													DontUse	Yes	No	Pct
AD	0	261	55	82.59%													0	279	38	88.01%
AF	2	108	13	89.26%													3	108	12	90.00%
AL	5	151	15	90.96%													5	152	15	91.02%
CF	0	64	13	83.12%													0	66	11	85.71%
CH	4	48	5	90.57%													4	50	4	92.59%
CS	0	20	1	95.24%													0	21	1	95.45%
EE	6	180	29	86.12%													6	180	29	86.12%
EG	10	316	81	79.60%													10	326	82	79.90%
EH	14	89	38	70.08%													14	99	29	77.34%
ES	8	135	21	86.54%													12	155	17	90.12%
FA	119	137	65	67.82%													119	148	57	72.20%
GN	9	96	27	78.05%													9	121	5	96.03%
HR	0	58	14	80.56%													0	69	6	92.00%
IC	1	172	17	91.01%													1	184	20	90.20%
LD	1	55	6	90.16%													2	59	6	90.77%
LS	7	249	27	90.22%													7	249	27	90.22%
MS	7	197	22	89.95%													7	193	22	89.77%
NE	1	144	11	92.90%													1	146	11	92.99%
NS	4	94	19	83.19%													5	109	14	88.62%
OP	0	12	2	85.71%													0	13	2	86.67%
PB	2	65	12	84.42%													2	82	13	86.32%
PH	3	105	21	83.33%													4	115	23	83.33%
Total	203	2756	514	84.28%													211	2924	444	86.82%

Question 11: Do you have a warning banner on all computers you are responsible for?

Answer: <http://www.lbl.gov/ITSD/Security/services/install-banner.html>

	10-29				0 - 50 Red	50 - 70 Yellow	70 - 100 Green	2-19			
DIV	DontUs	Yes	No	Pct				DontUse	Yes	No	Pct
AD	0	272	44	86.08%				0	276	41	87.07%
AF	3	102	18	85.00%				4	101	18	84.87%
AL	24	118	29	80.27%				24	119	29	80.41%
CF	0	72	5	93.51%				0	72	5	93.51%
CH	5	46	6	88.46%				5	47	6	88.68%
CS	0	21	0	100.00%				0	21	1	95.45%
EE	9	180	26	87.38%				9	180	26	87.38%
EG	13	345	49	87.56%				13	386	19	95.31%
EH	13	119	9	92.97%				13	121	8	93.80%
ES	6	133	25	84.18%				10	150	24	86.21%
FA	132	163	26	86.24%				132	165	27	85.94%
GN	9	106	17	86.18%				9	113	13	89.68%
HR	0	62	10	86.11%				0	69	6	92.00%
IC	1	178	11	94.18%				1	193	11	94.61%
LD	2	56	4	93.33%				3	60	4	93.75%
LS	11	228	44	83.82%				11	228	44	83.82%
MS	11	167	48	77.67%				11	163	48	77.25%
NE	0	146	10	93.59%				0	148	10	93.67%
NS	4	97	16	85.84%				5	105	18	85.37%
OP	0	13	1	92.86%				0	14	1	93.33%
PB	3	60	16	78.95%				3	76	18	80.85%
PH	6	104	19	84.55%				7	114	21	84.44%
Total	252	2788	433	86.56%				260	2921	398	88.01%

Question 12: Do you change your password according to the LBNL password policy?

Answer: <http://www.lbl.gov/ITSD/Security/guidelines/password.html>

	10-29				0 - 50 Red				50 - 70 Yellow				70 - 100 Green				2-19			
DIV	DontUse	Yes	No	Pct													DontUse	Yes	No	Pct
AD	0	302	14	95.57%													0	306	11	96.53%
AF	4	103	16	86.55%													5	102	16	86.44%
AL	16	128	27	82.58%													16	129	27	82.69%
CF	0	74	3	96.10%													0	74	3	96.10%
CH	5	50	2	96.15%													6	50	2	96.15%
CS	0	20	1	95.24%													0	21	1	95.45%
EE	6	188	21	89.95%													6	188	21	89.95%
EG	7	356	44	89.00%													7	373	38	90.75%
EH	16	113	12	90.40%													16	115	11	91.27%
ES	6	137	21	86.71%													10	154	20	88.51%
FA	134	175	12	93.58%													135	177	12	93.65%
GN	9	118	5	95.93%													9	124	2	98.41%
HR	0	68	4	94.44%													0	73	2	97.33%
IC	1	184	5	97.35%													1	199	5	97.55%
LD	2	52	8	86.67%													3	56	8	87.50%
LS	8	239	36	86.91%													8	239	36	86.91%
MS	11	176	39	81.86%													11	176	35	83.41%
NE	0	155	1	99.36%													0	157	1	99.37%
NS	3	93	21	81.58%													3	100	25	80.00%
OP	0	14	0	100.00%													0	15	0	100.00%
PB	2	65	12	84.42%													2	83	12	87.37%
PH	3	113	13	89.68%													4	124	14	89.86%
Total	233	2923	317	90.22%													242	3035	302	90.95%

Question 13: Is anti-virus software installed for all Macintosh or Windows computers you use?

Answer: <http://www.lbl.gov/ITSD/Security/vulnerabilities/virus.html>

10-29					0 - 60 Red					60 - 85 Yellow					85 - 100 Green					2-19				
DIV	DontUse	Yes	No	Pct											DontUse	Yes	No	Pct		DontUse	Yes	No	Pct	
AD	0	313	3	99.05%											0	314	3	99.05%						
AF	7	107	9	92.24%											7	107	9	92.24%						
AL	14	151	6	96.18%											14	152	6	96.20%						
CF	1	76	0	100.00%											1	76	0	100.00%						
CH	5	50	2	96.15%											5	51	2	96.23%						
CS	0	20	1	95.24%											0	21	1	95.45%						
EE	7	200	8	96.15%											7	200	8	96.15%						
EG	10	379	18	95.47%											10	393	15	96.32%						
EH	16	121	4	96.80%											17	121	4	96.80%						
ES	7	148	9	94.27%											10	165	9	94.83%						
FA	138	175	8	95.63%											139	178	7	96.22%						
GN	9	119	4	96.75%											9	124	2	98.41%						
HR	0	72	0	100.00%											0	75	0	100.00%						
IC	3	185	2	98.93%											3	197	5	97.52%						
LD	2	60	0	100.00%											3	64	0	100.00%						
LS	10	258	15	94.51%											10	258	15	94.51%						
MS	10	207	9	95.83%											9	204	9	95.77%						
NE	9	141	6	95.92%											9	143	6	95.97%						
NS	8	95	14	87.16%											9	104	15	87.39%						
OP	0	14	0	100.00%											0	15	0	100.00%						
PB	4	70	5	93.33%											4	88	5	94.62%						
PH	13	106	10	91.38%											16	113	13	89.68%						
Total	273	3067	133	95.84%											282	3163	134	95.94%						

Question 14: Do you know who your Computer Protection Liaison is?

Answer: <http://www.lbl.gov/ITSD/Security/people/cpic.html>

	10-29				0 - 50 Red				50 - 70 Yellow				70 - 100 Green				2-19			
DIV	DontUse	Yes	No	Pct													DontUse	Yes	No	Pct
AD	0	251	65	79.43%													0	260	57	82.02%
AF	4	83	36	69.75%													5	83	35	70.34%
AL	11	130	30	81.25%													11	131	30	81.37%
CF	0	46	31	59.74%													0	67	10	87.01%
CH	4	38	15	71.70%													4	40	14	74.07%
CS	0	17	4	80.95%													0	18	4	81.82%
EE	9	155	51	75.24%													9	155	51	75.24%
EG	11	278	118	70.20%													11	285	122	70.02%
EH	16	87	38	69.60%													16	97	29	76.98%
ES	6	128	30	81.01%													10	147	27	84.48%
FA	135	144	42	77.42%													136	149	39	79.26%
GN	9	97	26	78.86%													9	112	14	88.89%
HR	0	52	20	72.22%													0	59	16	78.67%
IC	1	172	17	91.01%													1	183	21	89.71%
LD	2	40	20	66.67%													3	44	20	68.75%
LS	10	215	58	78.75%													10	215	58	78.75%
MS	10	161	55	74.54%													10	158	54	74.53%
NE	0	132	24	84.62%													0	134	24	84.81%
NS	4	86	27	76.11%													5	96	27	78.05%
OP	0	13	1	92.86%													0	14	1	93.33%
PB	2	61	16	79.22%													2	76	19	80.00%
PH	3	95	31	75.40%													4	102	36	73.91%
Total	237	2481	755	76.67%													246	2625	708	78.76%

Question 15: Do you back up all information that you deem important to your work?

Answer: <http://www.lbl.gov/Workplace/RPM/R9.02.html#backups>

	10-29				0 - 50 Red				50 - 70 Yellow				70 - 100 Green				2-19			
DIV	DontUse	Yes	No	Pct													DontUse	Yes	No	Pct
AD	0	285	31	90.19%													0	287	30	90.54%
AF	4	112	7	94.12%													5	111	7	94.07%
AL	10	158	3	98.14%													10	159	3	98.15%
CF	0	70	7	90.91%													0	71	6	92.21%
CH	4	50	3	94.34%													4	52	2	96.30%
CS	0	20	1	95.24%													0	21	1	95.45%
EE	8	200	7	96.62%													8	200	7	96.62%
EG	13	354	40	89.85%													13	363	42	89.63%
EH	16	97	28	77.60%													16	101	25	80.16%
ES	7	147	10	93.63%													11	161	12	93.06%
FA	143	147	31	82.58%													143	149	32	82.32%
GN	10	99	23	81.15%													10	113	12	90.40%
HR	0	57	15	79.17%													0	62	13	82.67%
IC	1	183	6	96.83%													1	197	7	96.57%
LD	2	55	5	91.67%													3	59	5	92.19%
LS	9	255	19	93.07%													9	255	19	93.07%
MS	7	212	7	96.80%													7	208	7	96.74%
NE	0	152	4	97.44%													0	154	4	97.47%
NS	3	104	10	91.23%													4	114	10	91.94%
OP	0	14	0	100.00%													0	15	0	100.00%
PB	1	73	5	93.59%													1	90	6	93.75%
PH	3	119	7	94.44%													4	130	8	94.20%
Total	241	2963	269	91.68%													249	3072	258	92.25%

Question 16: Classified Information

Answer: http://isswdev/ISSM/definitions/prot_classified.html

	10-29			0 - 0 Green	0 - 0 Yellow	0 - 100 Red	2-19		
DIV	Total	Yes	Pct				Total	Yes	Pct
AD	315	1	0.32%				317	0	0.00%
AF	124	0	0.00%				123	0	0.00%
AL	174	1	0.57%				172	0	0.00%
CF	77	1	1.30%				77	0	0.00%
CH	59	0	0.00%				58	0	0.00%
CS	21	0	0.00%				22	0	0.00%
EE	214	0	0.00%				215	0	0.00%
EG	409	0	0.00%				418	0	0.00%
EH	136	1	0.74%				142	0	0.00%
ES	163	0	0.00%				184	0	0.00%
FA	331	9	2.72%				324	7	2.16%
GN	132	2	1.52%				135	0	0.00%
HR	72	0	0.00%				75	0	0.00%
IC	190	0	0.00%				205	0	0.00%
LD	62	0	0.00%				67	0	0.00%
LS	280	1	0.36%				283	0	0.00%
MS	225	1	0.44%				222	0	0.00%
NE	154	0	0.00%				158	0	0.00%
NS	115	0	0.00%				128	0	0.00%
OP	14	0	0.00%				15	0	0.00%
PB	78	0	0.00%				97	0	0.00%
PH	128	0	0.00%				142	0	0.00%
Total	3473	17	0.49%				3579	7	0.20%

Question 16: Unclassified Controlled Nuclear Information (UCNI)

Answer: http://isswdev/ISSM/definitions/prot_UCNI.html

	10-29			<i>0 - 0 Green</i>	<i>0 - 0 Yellow</i>	<i>0 - 100 Red</i>	2-19		
DIV	Total	Yes	Pct				Total	Yes	Pct
AD	315	0	0.00%				317	0	0.00%
AF	124	1	0.81%				123	0	0.00%
AL	174	4	2.30%				172	0	0.00%
CF	77	1	1.30%				77	0	0.00%
CH	59	0	0.00%				58	0	0.00%
CS	21	0	0.00%				22	0	0.00%
EE	214	0	0.00%				215	0	0.00%
EG	409	2	0.49%				418	0	0.00%
EH	136	0	0.00%				142	0	0.00%
ES	163	0	0.00%				184	0	0.00%
FA	331	3	0.91%				324	1	0.31%
GN	132	0	0.00%				135	0	0.00%
HR	72	0	0.00%				75	0	0.00%
IC	190	1	0.53%				205	0	0.00%
LD	62	0	0.00%				67	0	0.00%
LS	280	0	0.00%				283	0	0.00%
MS	225	0	0.00%				222	0	0.00%
NE	154	1	0.65%				158	0	0.00%
NS	115	0	0.00%				128	0	0.00%
OP	14	0	0.00%				15	0	0.00%
PB	78	0	0.00%				97	0	0.00%
PH	128	0	0.00%				142	0	0.00%
Total	3473	13	0.37%				3579	1	0.03%

Question 16: Naval Nuclear Propulsion (NNPI)**Answer:** http://isswdev/ISSM/definitions/prot_NNPI.html

	10-29			<i>0 - 0 Green</i>	<i>0 - 0 Yellow</i>	<i>0 - 100 Red</i>	2-19		
DIV	Total	Yes	Pct				Total	Yes	Pct
AD	315	1	0.32%				317	0	0.00%
AF	124	0	0.00%				123	0	0.00%
AL	174	1	0.57%				172	0	0.00%
CF	77	0	0.00%				77	0	0.00%
CH	59	0	0.00%				58	0	0.00%
CS	21	0	0.00%				22	0	0.00%
EE	214	0	0.00%				215	0	0.00%
EG	409	0	0.00%				418	0	0.00%
EH	136	0	0.00%				142	0	0.00%
ES	163	0	0.00%				184	0	0.00%
FA	331	0	0.00%				324	0	0.00%
GN	132	0	0.00%				135	0	0.00%
HR	72	0	0.00%				75	0	0.00%
IC	190	0	0.00%				205	0	0.00%
LD	62	0	0.00%				67	0	0.00%
LS	280	0	0.00%				283	0	0.00%
MS	225	0	0.00%				222	0	0.00%
NE	154	0	0.00%				158	0	0.00%
NS	115	0	0.00%				128	0	0.00%
OP	14	0	0.00%				15	0	0.00%
PB	78	0	0.00%				97	0	0.00%
PH	128	0	0.00%				142	0	0.00%
Total	3473	2	0.06%				3579	0	0.00%

Question 17: up to 10 seconds (Mission Critical)

Answer: http://isswdev/ISSM/definitions/prot_critical.html

	10-29			<i>0 - 0 Green</i>	<i>0 - 0 Yellow</i>	<i>0 - 100 Red</i>	2-19		
DIV	Total	Yes	Pct				Total	Yes	Pct
AD	315	0	0.00%				317	0	0.00%
AF	124	0	0.00%				123	0	0.00%
AL	174	0	0.00%				172	0	0.00%
CF	77	0	0.00%				77	0	0.00%
CH	59	0	0.00%				58	0	0.00%
CS	21	1	4.76%				22	0	0.00%
EE	214	0	0.00%				215	0	0.00%
EG	409	0	0.00%				418	0	0.00%
EH	136	0	0.00%				142	0	0.00%
ES	163	1	0.61%				184	0	0.00%
FA	331	4	1.21%				324	2	0.62%
GN	132	1	0.76%				135	0	0.00%
HR	72	0	0.00%				75	0	0.00%
IC	190	1	0.53%				205	0	0.00%
LD	62	0	0.00%				67	0	0.00%
LS	280	0	0.00%				283	0	0.00%
MS	225	0	0.00%				222	0	0.00%
NE	154	0	0.00%				158	0	0.00%
NS	115	0	0.00%				128	0	0.00%
OP	14	0	0.00%				15	0	0.00%
PB	78	0	0.00%				97	0	0.00%
PH	128	0	0.00%				142	0	0.00%
Total	3473	8	0.23%				3579	2	0.06%

Question 18: Additional comments or suggestions:

Question 1

Q1 has 2 answers depending upon your phone--your cell phone needs a different number from your Lab desk phone.

Question 4

Q4 needs an additional choice: "My building does not have card access."

Q4 is poorly designed -- it should have a N/A response.

Question 9

Q9 is 2 questions with 2 (possibly different) answers.

The link to RPM does not clarify who contact is.

The URL to #Q9 (workplace violence) is incorrect as link numbers have recently been revised. Please change URL to <http://www.lbl.gov/Workplace/RPM/R2.05.html#RTFTtoC25>.

Question 13

The answers to Q13 do not apply to me. I use computers, but not Windows or Macs.

Q13 presupposes the computer one uses requires anti-virus software.

Q13 does not really have the right answer for me in its multiple choice. I do use computers at work, I just don't use Windows or Macs.

Q13 is poorly worded for people who use computers that are neither Windows nor Macintosh.

No correct answer for Q13 because all the computers I use at work are Linux, but I could not submit the form without submitting an answer.

Q13, 16: N/A for computers not on a network or using "clean input" (formatted floppies, CD ROMs). These computers are where proprietary info is stored.

Question 14

Regarding Q 14, there is no "CCP Liaisons" attached.

CPP Liaison attachment didn't get here.

Question 16

I suggest a better link for Proprietary Information on Q16 is RPM 5.06(B)(1). Interested staff can then also learn about requirements for putting an NDA in place, so that we can help combat the all-too-frequent occurrence of unauthorized staff signing.

Question 17

Q17 should give examples of what you're talking about. I answered no simply because I don't think I have anything within my control that could cause millions of dollars in [damage].

Q17 is unclear. I work with HR data, Sensitive information. With identity theft and other problems with personal information, I don't quite know how to answer Q17.

I'm not clear about Q17. If you mean millions of dollars, then I'm probably not at risk. However, SS#, name & birth date can do damage in the thousands.

Answers to part 3 of question 17 need to be verified with the system owners.

I think question 17 is not written well and thus ambiguous.

Q17 is unintelligible.

Required system = PeopleSoft HRMS – payroll.

LBNL Website and A-Z Index

While so much more information is available using the A-Z on the web, it would be helpful to have a course on navigating LBNL websites.

The quantity of information is overwhelming... At least I know some Web pages exist. Finding them, when needed by a novice, is usually a problem from the LBL home page.

You've probably already done this, but ensure that all of the critical terms above are in the lab A-Z web index.

There is no way that I know of to find out this information when you need it, unless you are lucky and can guess what it is called in the main lab web directory. Do you seriously think anyone can remember all of it?

ISSM Website

The links provided were very useful to find the answer to the questions. It would be [useful] if they would be centralized somewhere.

Other

Thank you for providing the information links. It would be helpful if these information links were added to the employee self-service web page, https://hris.lbl.gov/self_service/.

Streamlining password requirements would be welcome; one password for all LBNL systems, changed yearly.

While I know how to access most items on the website, it wouldn't hurt to have these discussed during orientation.

Why not have a training class on this as part of all new employee training regardless of the number of hours a computer is used?

Please distribute information on the Crisis Action Team.

LBNL password policy is insecure.

Please establish a reminder system for changing LDAP passwords every six months. A simple e-mail with the password change URL would suffice. Thank you.

Appendix D

Performance Rating Criteria



INTEGRATED SAFEGUARDS & SECURITY MANAGEMENT

ERNEST ORLANDO LAWRENCE BERKELEY NATIONAL LABORATORY

2002 ISSM-Based Division Performance Criteria

ISSM Home

Take/Retake Questionnaire

Printable Questionnaire

Non-LDAP Questionnaire

View Division Profile ▶

View Division Performance

View Performance Criteria

Completed Survey

Not Completed Survey

Overview

Logout

Profile Statistic	Question used in survey to determine statistic	Criteria for Profile	Rating Criteria		
			Green	Yellow	Red
Employees in Division who have completed the Self-Assessment Questionnaire	Not Applicable	% of employees in the division that answered the questionnaire	>70%	>50% <69%	<50%
Classified Information Reported in Division	Do you work with classified information at LBNL?	% of employees who took the questionnaire that answered "Yes".	0%	N/A	>0%
UCNI Reported in Division	Do you work with UCNI at LBNL?	% of employees who took the questionnaire that answered "Yes".	0%	N/A	>0%
NNPI Reported in Division	Do you work with NNPI at LBNL?	% of employees who took the questionnaire that answered "Yes".	0%	N/A	>0%
Mission Critical Systems Reported in Division	Do you work with Mission Critical systems at LBNL?	% of employees who took the questionnaire that answered "Yes".	0%	N/A	>0%
Employees who know how to find the emergency phone number for the Laboratory	Do you know the emergency phone number for the Laboratory?	% of employees who took the questionnaire that answered "Yes".	>85%	>60% <85%	<60%
Employees who have access to the Employee Security Guide	Do you have access to the Employee Security Guide?	% of employees who took the questionnaire that answered "Yes".	>85%	>60% <85%	<60%
Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building	If a building has the new proximity card access system, do you know how to find the list of building authorizers in order to request access?	% of employees who took the questionnaire that answered "Yes".	>70%	>50% <69%	<50%

Employees who know how to request visitor access	Do you know how to request access for your visitors?	% of employees who took the questionnaire that answered "Yes".	>85%	>60% <85%	<60%
Employees who know whom to contact regarding keys to their office or building	Do you know whom to contact regarding keys to your office or building?	% of employees who took the questionnaire that answered "Yes".	>70%	>50% <69%	<50%
Employees who take appropriate measures to secure the property assigned to them	Do you take appropriate measures to secure the property assigned to you?	% of employees who took the questionnaire that answered "Yes".	>85%	>60% <85%	<60%
Security Access Managers who review their access lists annually	If you are a Security Access Manager , do you review your access lists annually?	Number of Security Access Managers in the division that have reviewed their access list.	100%	N/A	<100%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues	Are you aware of the Crisis Action Team and whom to contact regarding workplace violence concerns ?	% of employees who took the questionnaire that answered "Yes".	>70%	>50% <69%	<50%
Employees who know LBNL's legal requirements for obtaining software	Do you know the Lab's legal requirements for obtaining software?	% of employees who took the questionnaire that answered "Yes".	>85%	>60% <85%	<60%
Employees who have warning banners on all computers they are responsible for	Do you have a warning banner on all computers you are responsible for?	% of employees who took the questionnaire that answered "Yes".	>70%	>50% <69%	<50%
Employees who change their passwords according to the LBNL password policy	Do you change your password according to the LBNL password policy ?	% of employees who took the questionnaire that answered "Yes".	>70%	>50% <69%	<50%
Mac/PC desktops that have anti-virus software installed	Is anti-virus software installed for all Macintosh or Windows computers you use?	% of employees who took the questionnaire that answered "Yes".	>85%	>60% <85%	<60%
Employees who know who their CPP Liason is	Do you know who your Computer Protection	% of employees who took the questionnaire	>70%	>50% <69%	<50%

	Liaison is?	that answered "Yes".			
Employees who back up all information they deem important to their work	Do you back up all information that you deem important to your work?	% of employees who took the questionnaire that answered "Yes".	>70%	>50% <69%	<50%
Compromised systems that have been resolved	Not applicable. Comes from Computer Protection Program Data	% of computer compromises in the Division from <date1> to <date2>* that have been resolved.	>85%	<85% >60%	<60%
Vulnerable computers that have been resolved	Not applicable. Comes from Computer Protection Program Data	% of computers in the Division with vulnerabilities discovered between <date1> to <date2>* that have been resolved.	>70%	<70% >60%	<60%
Cracked passwords that have been changed	Not applicable. Comes from Computer Protection Program Data	% of employees in the division who have been notified <date1> to <date2>* that their passwords are weak, and have changed them.	>85%	<85% >60%	<60%

Appendix E

Organizational Profiles

This appendix presents the organizational profiles in alphabetical order.

Note: The organizational staff listed in the profiles were current at the time of the survey but in some cases have changed since then.



INTEGRATED SAFEGUARDS & SECURITY MANAGEMENT

ERNEST ORLANDO LAWRENCE BERKELEY NATIONAL LABORATORY

Accelerator & Fusion Research

DIVISION INFORMATION

ISSM Home

Take/Retake Questionnaire

Printable Questionnaire

Non-LDAP Questionnaire

View Division Profile ▶

View Division Performance

View Performance Criteria

Completed Survey

Not Completed Survey

Overview

Logout

Division Director: Barletta, William A

ISSM Liaison: Freeman, John C

CPP Liaison: Chew, Joseph T















Security Access Managers: Kono, Joy N

Employees in Division
([as surveyed](#)): 127

RATED STATISTICS

Click on colored square to view question and performance criteria.

Results of Survey Questions			
	Emps.	Rating	% Division Emps.
Employees in Division who have completed the Self-Assessment Questionnaire:	123		96.85%
	Emps.	Rating	% Took Survey
Classified Information reported in Division:	0		0%
UCNI reported in Division:	0		0%
NNPI reported in Division:	0		0%
Mission Critical Systems reported in Division:	0		0%
Employees who know the emergency phone number for the Laboratory :	119		96.75%
Employees who have access to the Employee Security Guide :	112		91.05%
Employees who know how to find the list of building authorizers if access is required to			

a proximity card-enabled building:	86		69.9%
Employees who know how to request visitor access :	113		91.85%
Employees who know whom to contact regarding keys to their office or building:	119		96.75%
Employees who take appropriate measures to secure the property assigned to them:	121		98.35%
Security Access Managers who review their access lists annually:	1		100%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues :	82		66.65%
Employees who know LBNL's legal requirements for obtaining software:	108		90%
Employees who have warning banners on all computers they are responsible for:	101		84.85%
Employees who change their passwords according to the LBNL password policy :	102		86.4%
Mac/PC desktops that have anti-virus software installed :	107		92.2%
Employees who know who their CPP Liaison is:	83		70.3%
Employees who back up all information they deem important to their work:	111		94.05%
Other Rated Security Data			
	Total #	Rating	Percent Fixed
Vulnerable computers that have been resolved (in 2002)	33		100%
Cracked passwords that have been changed (in 2002)	5		100%

INFORMATIONAL STATISTICS

Results of Questionnaire	
Employees who are known to have a security clearance :	8
Employees who answered "Yes" to the question, "Do you hold a security clearance that allows access to classified information?":	17
Proprietary Information reported in Division:	13
Personal Medical Information reported in Division:	1
Essential Systems reported in Division:	0
Required Systems reported in Division:	0
Number of employees who say they don't use a computer in the Division:	7
Other Security Data	
Thefts that have been reported in the Division (in 2002):	0

Thefts that have been reported at the Lab (in 2002):	10
Computers that have been compromised in the Division (in 2002):	1
Computers that have been compromised at the Lab (in 2002):	99
Instances of unacceptable computer use in the Division (in 2002):	4
Instances of unacceptable computer use at the Lab (in 2002):	217



INTEGRATED SAFEGUARDS & SECURITY MANAGEMENT

ERNEST ORLANDO LAWRENCE BERKELEY NATIONAL LABORATORY

Administrative Services

DIVISION INFORMATION

[ISSM Home](#)

[Take/Retake Questionnaire](#)

[Printable Questionnaire](#)

[Non-LDAP Questionnaire](#)

[View Division Profile](#) ▶

[View Division Performance](#)

[View Performance Criteria](#)

[Completed Survey](#)

[Not Completed Survey](#)

[Overview](#)

[Logout](#)

Division Director: More, Anil V

ISSM Liaison: Saucier, Elizabeth C

CPP Liaison: Clary, Mary M















Security Access Managers: Saucier, Elizabeth C

Employees in Division
([as surveyed](#)): 330

RATED STATISTICS

Click on colored square to view question and performance criteria.

Results of Survey Questions			
	Emps.	Rating	% Division Emps.
Employees in Division who have completed the Self-Assessment Questionnaire:	317		96.05%
	Emps.	Rating	% Took Survey
Classified Information reported in Division:	0		0%
UCNI reported in Division:	0		0%
NNPI reported in Division:	0		0%
Mission Critical Systems reported in Division:	0		0%
Employees who know the emergency phone number for the Laboratory :	304		95.9%
Employees who have access to the Employee Security Guide :	291		91.8%
Employees who know how to find the list of building authorizers if access is required to			

a proximity card-enabled building:	265		83.6%
Employees who know how to request visitor access :	310		97.75%
Employees who know whom to contact regarding keys to their office or building:	306		96.5%
Employees who take appropriate measures to secure the property assigned to them:	312		98.4%
Security Access Managers who review their access lists annually:	1		100%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues :	252		79.5%
Employees who know LBNL's legal requirements for obtaining software:	279		88%
Employees who have warning banners on all computers they are responsible for:	276		87.05%
Employees who change their passwords according to the LBNL password policy :	306		96.5%
Mac/PC desktops that have anti-virus software installed :	314		99.05%
Employees who know who their CPP Liaison is:	260		82%
Employees who back up all information they deem important to their work:	287		90.5%
Other Rated Security Data			
	Total #	Rating	Percent Fixed
Vulnerable computers that have been resolved (in 2002)	1		100%
Cracked passwords that have been changed (in 2002)	0		100%

INFORMATIONAL STATISTICS

Results of Questionnaire	
Employees who are known to have a security clearance :	0
Employees who answered "Yes" to the question, "Do you hold a security clearance that allows access to classified information?":	3
Proprietary Information reported in Division:	14
Personal Medical Information reported in Division:	12
Essential Systems reported in Division:	0
Required Systems reported in Division:	2
Number of employees who say they don't use a computer in the Division:	0
Other Security Data	
Thefts that have been reported in the Division (in 2002):	0

Thefts that have been reported at the Lab (in 2002):	10
Computers that have been compromised in the Division (in 2002):	0
Computers that have been compromised at the Lab (in 2002):	99
Instances of unacceptable computer use in the Division (in 2002):	3
Instances of unacceptable computer use at the Lab (in 2002):	217



INTEGRATED SAFEGUARDS & SECURITY MANAGEMENT

ERNEST ORLANDO LAWRENCE BERKELEY NATIONAL LABORATORY

Advanced Light Source

DIVISION INFORMATION

[ISSM Home](#)

[Take/Retake Questionnaire](#)

[Printable Questionnaire](#)

[Non-LDAP Questionnaire](#)

[View Division Profile](#) ▶

[View Division Performance](#)

[View Performance Criteria](#)

[Completed Survey](#)

[Not Completed Survey](#)

[Overview](#)

[Logout](#)

Division Director: Chemla, Daniel S

ISSM Liaison: Dixon, Bernadette B

CPP Liaison: McDonald, James L















Security Access Managers: Denlinger, Jonathan
Troutman, Jeffrey

Employees in Division
([as surveyed](#)): 203

RATED STATISTICS

Click on colored square to view question and performance criteria.

Results of Survey Questions			
	Emps.	Rating	% Division Emps.
Employees in Division who have completed the Self-Assessment Questionnaire:	172		84.7%
	Emps.	Rating	% Took Survey
Classified Information reported in Division:	0		0%
UCNI reported in Division:	0		0%
NNPI reported in Division:	0		0%
Mission Critical Systems reported in Division:	0		0%
Employees who know the emergency phone number for the Laboratory :	163		94.75%
Employees who have access to the Employee Security Guide :	145		84.3%

Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building:	144		83.7%
Employees who know how to request visitor access :	159		92.4%
Employees who know whom to contact regarding keys to their office or building:	162		94.15%
Employees who take appropriate measures to secure the property assigned to them:	172		100%
Security Access Managers who review their access lists annually:	2		100%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues :	140		81.4%
Employees who know LBNL's legal requirements for obtaining software:	152		91%
Employees who have warning banners on all computers they are responsible for:	119		80.4%
Employees who change their passwords according to the LBNL password policy :	129		82.65%
Mac/PC desktops that have anti-virus software installed :	152		96.2%
Employees who know who their CPP Liaison is:	131		81.35%
Employees who back up all information they deem important to their work:	159		98.15%
Other Rated Security Data			
	Total #	Rating	Percent Fixed
Vulnerable computers that have been resolved (in 2002)	85		100%
Cracked passwords that have been changed (in 2002)	0		100%

INFORMATIONAL STATISTICS

Results of Questionnaire	
Employees who are known to have a security clearance :	0
Employees who answered "Yes" to the question, "Do you hold a security clearance that allows access to classified information?":	8
Proprietary Information reported in Division:	26
Personal Medical Information reported in Division:	5
Essential Systems reported in Division:	0
Required Systems reported in Division:	0
Number of employees who say they don't use a computer in the Division:	27
Other Security Data	

Thefts that have been reported in the Division (in 2002):	1
Thefts that have been reported at the Lab (in 2002):	10
Computers that have been compromised in the Division (in 2002):	8
Computers that have been compromised at the Lab (in 2002):	99
Instances of unacceptable computer use in the Division (in 2002):	17
Instances of unacceptable computer use at the Lab (in 2002):	217



INTEGRATED SAFEGUARDS & SECURITY MANAGEMENT

ERNEST ORLANDO LAWRENCE BERKELEY NATIONAL LABORATORY

Chemical Sciences

DIVISION INFORMATION

ISSM Home

Take/Retake Questionnaire

Printable Questionnaire

Non-LDAP Questionnaire

View Division Profile ▶

View Division Performance

View Performance Criteria

Completed Survey

Not Completed Survey

Overview

Logout

Division Director: Neumark, Daniel M

ISSM Liaison: Prior, Michael H

CPP Liaison: Booth, Corwin H

Security Access Managers: Lukens Jr, Wayne W

Pettit, Robert S

Shuh, David K
















Employees in Division

([as surveyed](#)): 96

RATED STATISTICS

Click on colored square to view question and performance criteria.

Results of Survey Questions			
	Emps.	Rating	% Division Emps.
Employees in Division who have completed the Self-Assessment Questionnaire:	58		60.4%
	Emps.	Rating	% Took Survey
Classified Information reported in Division:	0		0%
UCNI reported in Division:	0		0%
NNPI reported in Division:	0		0%
Mission Critical Systems reported in Division:	0		0%
Employees who know the emergency phone number for the Laboratory :	54		93.1%

Employees who have access to the Employee Security Guide :	55		94.8%
Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building:	49		84.45%
Employees who know how to request visitor access :	52		89.65%
Employees who know whom to contact regarding keys to their office or building:	53		91.35%
Employees who take appropriate measures to secure the property assigned to them:	55		94.8%
Security Access Managers who review their access lists annually:	3		100%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues :	43		74.1%
Employees who know LBNL's legal requirements for obtaining software:	50		92.55%
Employees who have warning banners on all computers they are responsible for:	47		88.65%
Employees who change their passwords according to the LBNL password policy :	50		96.15%
Mac/PC desktops that have anti-virus software installed :	51		96.2%
Employees who know who their CPP Liaison is:	40		74.05%
Employees who back up all information they deem important to their work:	52		96.3%
Other Rated Security Data			
	Total #	Rating	Percent Fixed
Vulnerable computers that have been resolved (in 2002)	3		100%
Cracked passwords that have been changed (in 2002)	0		100%

INFORMATIONAL STATISTICS

Results of Questionnaire	
Employees who are known to have a security clearance :	0
Employees who answered "Yes" to the question, "Do you hold a security clearance that allows access to classified information?":	0
Proprietary Information reported in Division:	4
Personal Medical Information reported in Division:	1
Essential Systems reported in Division:	1
Required Systems reported in Division:	1
Number of employees who say they don't use a computer in the Division:	6

Other Security Data	
Thefts that have been reported in the Division (in 2002):	0
Thefts that have been reported at the Lab (in 2002):	10
Computers that have been compromised in the Division (in 2002):	0
Computers that have been compromised at the Lab (in 2002):	99
Instances of unacceptable computer use in the Division (in 2002):	3
Instances of unacceptable computer use at the Lab (in 2002):	217



INTEGRATED SAFEGUARDS & SECURITY MANAGEMENT

ERNEST ORLANDO LAWRENCE BERKELEY NATIONAL LABORATORY

Computing Sciences

DIVISION INFORMATION

[ISSM Home](#)

[Take/Retake Questionnaire](#)

[Printable Questionnaire](#)

[Non-LDAP Questionnaire](#)

[View Division Profile](#) ▶

[View Division Performance](#)

[View Performance Criteria](#)

[Completed Survey](#)

[Not Completed Survey](#)

[Overview](#)

[Logout](#)

Division Director: McCurdy,C William

ISSM Liaison: Ramsey,Dwayne

CPP Liaison: Manders,Chris J















Security Access Managers: Dooly,Martin K

Employees in Division
([as surveyed](#)): 31

RATED STATISTICS

Click on colored square to view question and performance criteria.

Results of Survey Questions			
	Emps.	Rating	% Division Emps.
Employees in Division who have completed the Self-Assessment Questionnaire:	22		70.95%
	Emps.	Rating	% Took Survey
Classified Information reported in Division:	0		0%
UCNI reported in Division:	0		0%
NNPI reported in Division:	0		0%
Mission Critical Systems reported in Division:	0		0%
Employees who know the emergency phone number for the Laboratory :	22		100%
Employees who have access to the Employee Security Guide :	22		100%
Employees who know how to find the list of building authorizers if access is required to			

a proximity card-enabled building:	20		90.9%
Employees who know how to request visitor access :	21		95.45%
Employees who know whom to contact regarding keys to their office or building:	19		86.35%
Employees who take appropriate measures to secure the property assigned to them:	22		100%
Security Access Managers who review their access lists annually:	1		100%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues :	17		77.25%
Employees who know LBNL's legal requirements for obtaining software:	21		95.45%
Employees who have warning banners on all computers they are responsible for:	21		95.45%
Employees who change their passwords according to the LBNL password policy :	21		95.45%
Mac/PC desktops that have anti-virus software installed :	21		95.45%
Employees who know who their CPP Liaison is:	18		81.8%
Employees who back up all information they deem important to their work:	21		95.45%
Other Rated Security Data			
	Total #	Rating	Percent Fixed
Vulnerable computers that have been resolved (in 2002)	90		100%
Cracked passwords that have been changed (in 2002)	303		100%

INFORMATIONAL STATISTICS

Results of Questionnaire	
Employees who are known to have a security clearance :	0
Employees who answered "Yes" to the question, "Do you hold a security clearance that allows access to classified information?":	2
Proprietary Information reported in Division:	1
Personal Medical Information reported in Division:	1
Essential Systems reported in Division:	1
Required Systems reported in Division:	1
Number of employees who say they don't use a computer in the Division:	0
Other Security Data	
Thefts that have been reported in the Division (in 2002):	0

Thefts that have been reported at the Lab (in 2002):	10
Computers that have been compromised in the Division (in 2002):	2
Computers that have been compromised at the Lab (in 2002):	99
Instances of unacceptable computer use in the Division (in 2002):	1
Instances of unacceptable computer use at the Lab (in 2002):	217



INTEGRATED SAFEGUARDS & SECURITY MANAGEMENT

ERNEST ORLANDO LAWRENCE BERKELEY NATIONAL LABORATORY

Earth Sciences

DIVISION INFORMATION

[ISSM Home](#)

[Take/Retake Questionnaire](#)

[Printable Questionnaire](#)

[Non-LDAP Questionnaire](#)

[View Division Profile](#) ▶

[View Division Performance](#)

[View Performance Criteria](#)

[Completed Survey](#)

[Not Completed Survey](#)

[Overview](#)

[Logout](#)

Division Director: Bodvarsson, Gudmundur S

ISSM Liaison: Wuy, Linda D

CPP Liaison: Kurtzer, Greg M
Lau, Peter K
















Security Access Managers: Hazen, Terry C
Holman, Hoi-Ying
Kramer, Bridget R

Employees in Division
([as surveyed](#)): 186

RATED STATISTICS

Click on colored square to view question and performance criteria.

Results of Survey Questions			
	Emps.	Rating	% Division Emps.
Employees in Division who have completed the Self-Assessment Questionnaire:	184		98.9%
	Emps.	Rating	% Took Survey
Classified Information reported in Division:	0		0%
UCNI reported in Division:	0		0%
NNPI reported in Division:	0		0%
Mission Critical Systems reported in Division:	0		0%
Employees who know the emergency phone number for the Laboratory :	179		97.25%

Employees who have access to the Employee Security Guide :	169		91.85%
Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building:	151		82.05%
Employees who know how to request visitor access :	175		95.1%
Employees who know whom to contact regarding keys to their office or building:	174		94.55%
Employees who take appropriate measures to secure the property assigned to them:	180		97.8%
Security Access Managers who review their access lists annually:	3		100%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues :	150		81.5%
Employees who know LBNL's legal requirements for obtaining software:	155		90.1%
Employees who have warning banners on all computers they are responsible for:	150		86.2%
Employees who change their passwords according to the LBNL password policy :	154		88.5%
Mac/PC desktops that have anti-virus software installed :	165		94.8%
Employees who know who their CPP Liaison is:	147		84.45%
Employees who back up all information they deem important to their work:	161		93.05%
Other Rated Security Data			
	Total #	Rating	Percent Fixed
Vulnerable computers that have been resolved (in 2002)	91		100%
Cracked passwords that have been changed (in 2002)	0		100%

INFORMATIONAL STATISTICS

Results of Questionnaire	
Employees who are known to have a security clearance :	3
Employees who answered "Yes" to the question, "Do you hold a security clearance that allows access to classified information?":	8
Proprietary Information reported in Division:	18
Personal Medical Information reported in Division:	1
Essential Systems reported in Division:	1
Required Systems reported in Division:	3
Number of employees who say they don't use a computer in the Division:	12

Other Security Data	
Thefts that have been reported in the Division (in 2002):	1
Thefts that have been reported at the Lab (in 2002):	10
Computers that have been compromised in the Division (in 2002):	4
Computers that have been compromised at the Lab (in 2002):	99
Instances of unacceptable computer use in the Division (in 2002):	5
Instances of unacceptable computer use at the Lab (in 2002):	217



INTEGRATED SAFEGUARDS & SECURITY MANAGEMENT

ERNEST ORLANDO LAWRENCE BERKELEY NATIONAL LABORATORY

Engineering

DIVISION INFORMATION

ISSM Home

Take/Retake Questionnaire

Printable Questionnaire

Non-LDAP Questionnaire

View Division Profile ▶

View Division Performance

View Performance Criteria

Completed Survey

Not Completed Survey

Overview

Logout

Division Director: Triplett, James T

ISSM Liaison: Wong, Weyland

CPP Liaison: Lawrence, Charles E

















Security Access Managers: Luke, Paul N
Palaio, Nicholas P
Paris, Karen M
Salmassi, Farhad
Wong, Weyland

Employees in Division
([as surveyed](#)): 421

RATED STATISTICS

Click on colored square to view question and performance criteria.

Results of Survey Questions			
	Emps.	Rating	% Division Emps.
Employees in Division who have completed the Self-Assessment Questionnaire:	418		99.25%
	Emps.	Rating	% Took Survey
Classified Information reported in Division:	0		0%
UCNI reported in Division:	0		0%
NNPI reported in Division:	0		0%
Mission Critical Systems reported in Division:	0		0%

Employees who know the emergency phone number for the Laboratory :	413		98.8%
Employees who have access to the Employee Security Guide :	372		89%
Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building:	308		73.65%
Employees who know how to request visitor access :	372		89%
Employees who know whom to contact regarding keys to their office or building:	393		94%
Employees who take appropriate measures to secure the property assigned to them:	418		100%
Security Access Managers who review their access lists annually:	5		100%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues :	265		63.4%
Employees who know LBNL's legal requirements for obtaining software:	326		79.9%
Employees who have warning banners on all computers they are responsible for:	386		95.3%
Employees who change their passwords according to the LBNL password policy :	373		90.75%
Mac/PC desktops that have anti-virus software installed :	393		96.3%
Employees who know who their CPP Liaison is:	285		70%
Employees who back up all information they deem important to their work:	363		89.6%
Other Rated Security Data			
	Total #	Rating	Percent Fixed
Vulnerable computers that have been resolved (in 2002)	56		100%
Cracked passwords that have been changed (in 2002)	116		94%

INFORMATIONAL STATISTICS

Results of Questionnaire	
Employees who are known to have a security clearance :	15
Employees who answered "Yes" to the question, "Do you hold a security clearance that allows access to classified information?":	20
Proprietary Information reported in Division:	53
Personal Medical Information reported in Division:	9
Essential Systems reported in Division:	2
Required Systems reported in Division:	5

Number of employees who say they don't use a computer in the Division:	15
Other Security Data	
Thefts that have been reported in the Division (in 2002):	1
Thefts that have been reported at the Lab (in 2002):	10
Computers that have been compromised in the Division (in 2002):	6
Computers that have been compromised at the Lab (in 2002):	99
Instances of unacceptable computer use in the Division (in 2002):	26
Instances of unacceptable computer use at the Lab (in 2002):	217



INTEGRATED SAFEGUARDS & SECURITY MANAGEMENT

ERNEST ORLANDO LAWRENCE BERKELEY NATIONAL LABORATORY

Environment, Health & Safety

DIVISION INFORMATION

[ISSM Home](#)

[Take/Retake Questionnaire](#)

[Printable Questionnaire](#)

[Non-LDAP Questionnaire](#)

[View Division Profile](#) ▶

[View Division Performance](#)

[View Performance Criteria](#)

[Completed Survey](#)

[Not Completed Survey](#)

[Overview](#)

[Logout](#)

Division Director: McGraw, David C

ISSM Liaison: Bell, Donald W

CPP Liaison: Abraham, Stephen B
Bell, Donald W

Security Access Managers: Bell, Donald W
Decastro, Theodore M
English, Gerald A
Floyd, James G
Grondona, Connie E
Rothermich, Nancy E
Sohner, Stephen L
Wong, June J

Employees in Division
([as surveyed](#)): 146

RATED STATISTICS

Click on colored square to view question and performance criteria.

Results of Survey Questions			
	Emps.	Rating	% Division Emps.
Employees in Division who have completed the Self-Assessment Questionnaire:	142		97.25%
	Emps.	Rating	% Took Survey
Classified Information reported in Division:	0		0%

UCNI reported in Division:	0		0%
NNPI reported in Division:	0		0%
Mission Critical Systems reported in Division:	0		0%
Employees who know the emergency phone number for the Laboratory :	140		98.55%
Employees who have access to the Employee Security Guide :	131		92.25%
Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building:	117		82.35%
Employees who know how to request visitor access :	131		92.25%
Employees who know whom to contact regarding keys to their office or building:	134		94.35%
Employees who take appropriate measures to secure the property assigned to them:	142		100%
Security Access Managers who review their access lists annually:	8		100%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues :	109		76.75%
Employees who know LBNL's legal requirements for obtaining software:	99		77.3%
Employees who have warning banners on all computers they are responsible for:	121		93.8%
Employees who change their passwords according to the LBNL password policy :	115		91.25%
Mac/PC desktops that have anti-virus software installed :	121		96.8%
Employees who know who their CPP Liaison is:	97		76.95%
Employees who back up all information they deem important to their work:	101		80.15%
Other Rated Security Data			
	Total #	Rating	Percent Fixed
Vulnerable computers that have been resolved (in 2002)	9		100%
Cracked passwords that have been changed (in 2002)	44		100%

INFORMATIONAL STATISTICS

Results of Questionnaire	
Employees who are known to have a security clearance :	1
Employees who answered "Yes" to the question, "Do you hold a security clearance that allows access to classified information?":	3
Proprietary Information reported in Division:	11

Personal Medical Information reported in Division:	20
Essential Systems reported in Division:	3
Required Systems reported in Division:	6
Number of employees who say they don't use a computer in the Division:	18
Other Security Data	
Thefts that have been reported in the Division (in 2002):	0
Thefts that have been reported at the Lab (in 2002):	10
Computers that have been compromised in the Division (in 2002):	0
Computers that have been compromised at the Lab (in 2002):	99
Instances of unacceptable computer use in the Division (in 2002):	6
Instances of unacceptable computer use at the Lab (in 2002):	217



INTEGRATED SAFEGUARDS & SECURITY MANAGEMENT

ERNEST ORLANDO LAWRENCE BERKELEY NATIONAL LABORATORY

Environmental Energy Tech.

DIVISION INFORMATION

[ISSM Home](#)

[Take/Retake Questionnaire](#)

[Printable Questionnaire](#)

[Non-LDAP Questionnaire](#)

[View Division Profile](#) ▶

[View Division Performance](#)

[View Performance Criteria](#)

[Completed Survey](#)

[Not Completed Survey](#)

[Overview](#)

[Logout](#)

Division Director: Levine, Mark D

ISSM Liaison: Lucas, Donald

CPP Liaison: Revzan, Kenneth L















Security Access Managers: Cordell, Joyce D

Employees in Division
([as surveyed](#)): 308

RATED STATISTICS

Click on colored square to view question and performance criteria.

Results of Survey Questions			
	Emps.	Rating	% Division Emps.
Employees in Division who have completed the Self-Assessment Questionnaire:	215		69.8%
	Emps.	Rating	% Took Survey
Classified Information reported in Division:	0		0%
UCNI reported in Division:	0		0%
NNPI reported in Division:	0		0%
Mission Critical Systems reported in Division:	0		0%
Employees who know the emergency phone number for the Laboratory :	200		93%
Employees who have access to the Employee Security Guide :	194		90.2%
Employees who know how to find the list of building authorizers if access is required to			

a proximity card-enabled building:	175		81.4%
Employees who know how to request visitor access :	206		95.8%
Employees who know whom to contact regarding keys to their office or building:	197		91.6%
Employees who take appropriate measures to secure the property assigned to them:	209		97.2%
Security Access Managers who review their access lists annually:	1		100%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues :	144		66.95%
Employees who know LBNL's legal requirements for obtaining software:	180		86.1%
Employees who have warning banners on all computers they are responsible for:	180		87.35%
Employees who change their passwords according to the LBNL password policy :	188		89.95%
Mac/PC desktops that have anti-virus software installed :	200		96.15%
Employees who know who their CPP Liaison is:	155		75.2%
Employees who back up all information they deem important to their work:	200		96.6%
Other Rated Security Data			
	Total #	Rating	Percent Fixed
Vulnerable computers that have been resolved (in 2002)	150		100%
Cracked passwords that have been changed (in 2002)	197		100%

INFORMATIONAL STATISTICS

Results of Questionnaire	
Employees who are known to have a security clearance :	4
Employees who answered "Yes" to the question, "Do you hold a security clearance that allows access to classified information?":	10
Proprietary Information reported in Division:	46
Personal Medical Information reported in Division:	3
Essential Systems reported in Division:	1
Required Systems reported in Division:	5
Number of employees who say they don't use a computer in the Division:	9
Other Security Data	
Thefts that have been reported in the Division (in 2002):	1

Thefts that have been reported at the Lab (in 2002):	10
Computers that have been compromised in the Division (in 2002):	14
Computers that have been compromised at the Lab (in 2002):	99
Instances of unacceptable computer use in the Division (in 2002):	19
Instances of unacceptable computer use at the Lab (in 2002):	217



INTEGRATED SAFEGUARDS & SECURITY MANAGEMENT

ERNEST ORLANDO LAWRENCE BERKELEY NATIONAL LABORATORY

Facilities

DIVISION INFORMATION

ISSM Home

- Take/Retake Questionnaire
- Printable Questionnaire
- Non-LDAP Questionnaire

- View Division Profile ▶
- View Division Performance
- View Performance Criteria

- Completed Survey
- Not Completed Survey

Overview

Logout

Division Director: Camper, J.R
Reyes, George D

ISSM Liaison: Huynh, Chinh
Pon, John

CPP Liaison: Pon, John





















Security Access Managers: Berninzoni, Robert A
Llewellyn, William E
McPherson, David L
Murphy, James W
Pon, John
Reese Jr, Thomas A
Rosas, George A
Trigales, Kevin P
Weber, Donald F
Wu, William H

Employees in Division
([as surveyed](#)): 337

RATED STATISTICS

Click on colored square to view question and performance criteria.

Results of Survey Questions			
	Emps.	Rating	% Division Emps.
Employees in Division who have completed the Self-Assessment Questionnaire:	324		96.1%
			% Took

	Emps.	Rating	Survey
Classified Information reported in Division:	7		2.15%
UCNI reported in Division:	1		0.3%
NNPI reported in Division:	0		0%
Mission Critical Systems reported in Division:	2		0.6%
Employees who know the emergency phone number for the Laboratory :	311		95.95%
Employees who have access to the Employee Security Guide :	268		82.7%
Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building:	237		73.15%
Employees who know how to request visitor access :	266		82.1%
Employees who know whom to contact regarding keys to their office or building:	308		95.05%
Employees who take appropriate measures to secure the property assigned to them:	315		97.2%
Security Access Managers who review their access lists annually:	7		70%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues :	211		65.1%
Employees who know LBNL's legal requirements for obtaining software:	148		72.2%
Employees who have warning banners on all computers they are responsible for:	165		85.9%
Employees who change their passwords according to the LBNL password policy :	177		93.65%
Mac/PC desktops that have anti-virus software installed :	178		96.2%
Employees who know who their CPP Liaison is:	149		79.25%
Employees who back up all information they deem important to their work:	149		82.3%
Other Rated Security Data			
	Total #	Rating	Percent Fixed
Vulnerable computers that have been resolved (in 2002)	7		100%
Cracked passwords that have been changed (in 2002)	0		100%

INFORMATIONAL STATISTICS

Results of Questionnaire	
Employees who are known to have a security clearance :	2
Employees who answered "Yes" to the question, "Do you hold a security clearance that allows access to	

classified information?":	17
Proprietary Information reported in Division:	14
Personal Medical Information reported in Division:	8
Essential Systems reported in Division:	7
Required Systems reported in Division:	8
Number of employees who say they don't use a computer in the Division:	146
Other Security Data	
Thefts that have been reported in the Division (in 2002):	1
Thefts that have been reported at the Lab (in 2002):	10
Computers that have been compromised in the Division (in 2002):	2
Computers that have been compromised at the Lab (in 2002):	99
Instances of unacceptable computer use in the Division (in 2002):	10
Instances of unacceptable computer use at the Lab (in 2002):	217



INTEGRATED SAFEGUARDS & SECURITY MANAGEMENT

ERNEST ORLANDO LAWRENCE BERKELEY NATIONAL LABORATORY

Financial Services

DIVISION INFORMATION

ISSM Home

Take/Retake Questionnaire

Printable Questionnaire

Non-LDAP Questionnaire

View Division Profile ▶

View Division Performance

View Performance Criteria

Completed Survey

Not Completed Survey

Overview

Logout

Division Director: Wasson, William A

ISSM Liaison: Bell, Andre R

CPP Liaison: Speros, John P















Security Access Managers: Brown, Linda L

Employees in Division
([as surveyed](#)): 80

RATED STATISTICS

Click on colored square to view question and performance criteria.

Results of Survey Questions			
	Emps.	Rating	% Division Emps.
Employees in Division who have completed the Self-Assessment Questionnaire:	77		96.25%
	Emps.	Rating	% Took Survey
Classified Information reported in Division:	0		0%
UCNI reported in Division:	0		0%
NNPI reported in Division:	0		0%
Mission Critical Systems reported in Division:	0		0%
Employees who know the emergency phone number for the Laboratory :	75		97.4%
Employees who have access to the Employee Security Guide :	74		96.1%
Employees who know how to find the list of building authorizers if access is required to			

a proximity card-enabled building:	53		68.8%
Employees who know how to request visitor access :	61		79.2%
Employees who know whom to contact regarding keys to their office or building:	75		97.4%
Employees who take appropriate measures to secure the property assigned to them:	74		96.1%
Security Access Managers who review their access lists annually:	1		100%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues :	45		58.4%
Employees who know LBNL's legal requirements for obtaining software:	66		85.7%
Employees who have warning banners on all computers they are responsible for:	72		93.5%
Employees who change their passwords according to the LBNL password policy :	74		96.1%
Mac/PC desktops that have anti-virus software installed :	76		100%
Employees who know who their CPP Liaison is:	67		87%
Employees who back up all information they deem important to their work:	71		92.2%
Other Rated Security Data			
	Total #	Rating	Percent Fixed
Vulnerable computers that have been resolved (in 2002)	1		100%
Cracked passwords that have been changed (in 2002)	0		100%

INFORMATIONAL STATISTICS

Results of Questionnaire	
Employees who are known to have a security clearance :	0
Employees who answered "Yes" to the question, "Do you hold a security clearance that allows access to classified information?":	2
Proprietary Information reported in Division:	22
Personal Medical Information reported in Division:	4
Essential Systems reported in Division:	5
Required Systems reported in Division:	9
Number of employees who say they don't use a computer in the Division:	1
Other Security Data	
Thefts that have been reported in the Division (in 2002):	0

Thefts that have been reported at the Lab (in 2002):	10
Computers that have been compromised in the Division (in 2002):	0
Computers that have been compromised at the Lab (in 2002):	99
Instances of unacceptable computer use in the Division (in 2002):	3
Instances of unacceptable computer use at the Lab (in 2002):	217



INTEGRATED SAFEGUARDS & SECURITY MANAGEMENT

ERNEST ORLANDO LAWRENCE BERKELEY NATIONAL LABORATORY

Genomics Division

DIVISION INFORMATION

ISSM Home

Take/Retake Questionnaire

Printable Questionnaire

Non-LDAP Questionnaire

View Division Profile ▶

View Division Performance

View Performance Criteria

Completed Survey

Not Completed Survey

Overview

Logout

Division Director: Rubin,Edward M

ISSM Liaison: Wenning,Sarah

CPP Liaison: Yumae,Brian S















Security Access Managers: Wenning,Sarah

Employees in Division
([as surveyed](#)): 139

RATED STATISTICS

Click on colored square to view question and performance criteria.

Results of Survey Questions			
	Emps.	Rating	% Division Emps.
Employees in Division who have completed the Self-Assessment Questionnaire:	135		97.1%
	Emps.	Rating	% Took Survey
Classified Information reported in Division:	0		0%
UCNI reported in Division:	0		0%
NNPI reported in Division:	0		0%
Mission Critical Systems reported in Division:	0		0%
Employees who know the emergency phone number for the Laboratory :	127		94.05%
Employees who have access to the Employee Security Guide :	127		94.05%
Employees who know how to find the list of building authorizers if access is required to			

a proximity card-enabled building:	112		82.95%
Employees who know how to request visitor access :	127		94.05%
Employees who know whom to contact regarding keys to their office or building:	132		97.75%
Employees who take appropriate measures to secure the property assigned to them:	134		99.25%
Security Access Managers who review their access lists annually:	1		100%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues :	110		81.45%
Employees who know LBNL's legal requirements for obtaining software:	121		96%
Employees who have warning banners on all computers they are responsible for:	113		89.65%
Employees who change their passwords according to the LBNL password policy :	124		98.4%
Mac/PC desktops that have anti-virus software installed :	124		98.4%
Employees who know who their CPP Liaison is:	112		88.85%
Employees who back up all information they deem important to their work:	113		90.4%
Other Rated Security Data			
	Total #	Rating	Percent Fixed
Vulnerable computers that have been resolved (in 2002)	57		100%
Cracked passwords that have been changed (in 2002)	32		91%

INFORMATIONAL STATISTICS

Results of Questionnaire	
Employees who are known to have a security clearance :	0
Employees who answered "Yes" to the question, "Do you hold a security clearance that allows access to classified information?":	6
Proprietary Information reported in Division:	11
Personal Medical Information reported in Division:	2
Essential Systems reported in Division:	2
Required Systems reported in Division:	5
Number of employees who say they don't use a computer in the Division:	11
Other Security Data	
Thefts that have been reported in the Division (in 2002):	0

Thefts that have been reported at the Lab (in 2002):	10
Computers that have been compromised in the Division (in 2002):	1
Computers that have been compromised at the Lab (in 2002):	99
Instances of unacceptable computer use in the Division (in 2002):	0
Instances of unacceptable computer use at the Lab (in 2002):	217



INTEGRATED SAFEGUARDS & SECURITY MANAGEMENT

ERNEST ORLANDO LAWRENCE BERKELEY NATIONAL LABORATORY

Human Resources

DIVISION INFORMATION

[ISSM Home](#)

[Take/Retake Questionnaire](#)

[Printable Questionnaire](#)

[Non-LDAP Questionnaire](#)

[View Division Profile](#) ▶

[View Division Performance](#)

[View Performance Criteria](#)

[Completed Survey](#)

[Not Completed Survey](#)

[Overview](#)

[Logout](#)

Division Director: Scott,Randolph R

ISSM Liaison: Coolahan,Cynthia C

CPP Liaison: Guerrero,Daisy C















Security Access Managers: Attia,Diana M

Employees in Division
([as surveyed](#)): 76

RATED STATISTICS

Click on colored square to view question and performance criteria.

Results of Survey Questions			
	Emps.	Rating	% Division Emps.
Employees in Division who have completed the Self-Assessment Questionnaire:	75		98.65%
	Emps.	Rating	% Took Survey
Classified Information reported in Division:	0		0%
UCNI reported in Division:	0		0%
NNPI reported in Division:	0		0%
Mission Critical Systems reported in Division:	0		0%
Employees who know the emergency phone number for the Laboratory :	74		98.65%
Employees who have access to the Employee Security Guide :	72		96%
Employees who know how to find the list of building authorizers if access is required to			

a proximity card-enabled building:	62		82.65%
Employees who know how to request visitor access :	74		98.65%
Employees who know whom to contact regarding keys to their office or building:	73		97.3%
Employees who take appropriate measures to secure the property assigned to them:	73		97.3%
Security Access Managers who review their access lists annually:	1		100%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues :	56		74.65%
Employees who know LBNL's legal requirements for obtaining software:	69		92%
Employees who have warning banners on all computers they are responsible for:	69		92%
Employees who change their passwords according to the LBNL password policy :	73		97.3%
Mac/PC desktops that have anti-virus software installed :	75		100%
Employees who know who their CPP Liaison is:	59		78.65%
Employees who back up all information they deem important to their work:	62		82.65%
Other Rated Security Data			
	Total #	Rating	Percent Fixed
Vulnerable computers that have been resolved (in 2002)	0		100%
Cracked passwords that have been changed (in 2002)	0		100%

INFORMATIONAL STATISTICS

Results of Questionnaire	
Employees who are known to have a security clearance :	0
Employees who answered "Yes" to the question, "Do you hold a security clearance that allows access to classified information?":	0
Proprietary Information reported in Division:	4
Personal Medical Information reported in Division:	13
Essential Systems reported in Division:	1
Required Systems reported in Division:	3
Number of employees who say they don't use a computer in the Division:	0
Other Security Data	
Thefts that have been reported in the Division (in 2002):	0

Thefts that have been reported at the Lab (in 2002):	10
Computers that have been compromised in the Division (in 2002):	0
Computers that have been compromised at the Lab (in 2002):	99
Instances of unacceptable computer use in the Division (in 2002):	3
Instances of unacceptable computer use at the Lab (in 2002):	217



INTEGRATED SAFEGUARDS & SECURITY MANAGEMENT

ERNEST ORLANDO LAWRENCE BERKELEY NATIONAL LABORATORY

Info. Technologies & Services

DIVISION INFORMATION

ISSM Home

Take/Retake Questionnaire

Printable Questionnaire

Non-LDAP Questionnaire

View Division Profile ▶

View Division Performance

View Performance Criteria

Completed Survey

Not Completed Survey

Overview

Logout

Division Director: Merola,Alexander X

ISSM Liaison: Ramsey,Dwayne

CPP Liaison: Manders,Chris J
















Security Access Managers: Dooly,Martin K
Kapus,George
Seidler,Ellen D

Employees in Division
([as surveyed](#)): 227

RATED STATISTICS

Click on colored square to view question and performance criteria.

Results of Survey Questions			
	Emps.	Rating	% Division Emps.
Employees in Division who have completed the Self-Assessment Questionnaire:	205		90.3%
	Emps.	Rating	% Took Survey
Classified Information reported in Division:	0		0%
UCNI reported in Division:	0		0%
NNPI reported in Division:	0		0%
Mission Critical Systems reported in Division:	0		0%
Employees who know the emergency phone number for the Laboratory :	199		97.05%

Employees who have access to the Employee Security Guide :	191		93.15%
Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building:	175		85.35%
Employees who know how to request visitor access :	194		94.6%
Employees who know whom to contact regarding keys to their office or building:	197		96.1%
Employees who take appropriate measures to secure the property assigned to them:	203		99%
Security Access Managers who review their access lists annually:	3		100%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues :	152		74.15%
Employees who know LBNL's legal requirements for obtaining software:	184		90.2%
Employees who have warning banners on all computers they are responsible for:	193		94.6%
Employees who change their passwords according to the LBNL password policy :	199		97.55%
Mac/PC desktops that have anti-virus software installed :	197		97.5%
Employees who know who their CPP Liaison is:	183		89.7%
Employees who back up all information they deem important to their work:	197		96.55%
Other Rated Security Data			
	Total #	Rating	Percent Fixed
Vulnerable computers that have been resolved (in 2002)	64		100%
Cracked passwords that have been changed (in 2002)	312		100%

INFORMATIONAL STATISTICS

Results of Questionnaire	
Employees who are known to have a security clearance :	3
Employees who answered "Yes" to the question, "Do you hold a security clearance that allows access to classified information?":	5
Proprietary Information reported in Division:	35
Personal Medical Information reported in Division:	12
Essential Systems reported in Division:	12
Required Systems reported in Division:	28
Number of employees who say they don't use a computer in the Division:	3

Other Security Data	
Thefts that have been reported in the Division (in 2002):	1
Thefts that have been reported at the Lab (in 2002):	10
Computers that have been compromised in the Division (in 2002):	12
Computers that have been compromised at the Lab (in 2002):	99
Instances of unacceptable computer use in the Division (in 2002):	16
Instances of unacceptable computer use at the Lab (in 2002):	217



INTEGRATED SAFEGUARDS & SECURITY MANAGEMENT

ERNEST ORLANDO LAWRENCE BERKELEY NATIONAL LABORATORY

Laboratory Directorate

DIVISION INFORMATION

[ISSM Home](#)

[Take/Retake Questionnaire](#)

[Printable Questionnaire](#)

[Non-LDAP Questionnaire](#)

[View Division Profile](#) ▶

[View Division Performance](#)

[View Performance Criteria](#)

[Completed Survey](#)

[Not Completed Survey](#)

[Overview](#)

[Logout](#)

Division Director: Shank, Charles V

ISSM Liaison: Bear, Guy

Magee, Janice A

CPP Liaison: Tallarico, Nancy J

Security Access Managers: Magee, Janice A















Employees in Division

([as surveyed](#)): 69

RATED STATISTICS

Click on colored square to view question and performance criteria.

Results of Survey Questions			
	Emps.	Rating	% Division Emps.
Employees in Division who have completed the Self-Assessment Questionnaire:	67		97.1%
	Emps.	Rating	% Took Survey
Classified Information reported in Division:	0		0%
UCNI reported in Division:	0		0%
NNPI reported in Division:	0		0%
Mission Critical Systems reported in Division:	0		0%
Employees who know the emergency phone number for the Laboratory :	62		92.5%
Employees who have access to the Employee Security Guide :	63		94%

Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building:	53		79.1%
Employees who know how to request visitor access :	62		92.5%
Employees who know whom to contact regarding keys to their office or building:	59		88.05%
Employees who take appropriate measures to secure the property assigned to them:	66		98.5%
Security Access Managers who review their access lists annually:	1		100%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues :	45		67.15%
Employees who know LBNL's legal requirements for obtaining software:	59		90.75%
Employees who have warning banners on all computers they are responsible for:	60		93.75%
Employees who change their passwords according to the LBNL password policy :	56		87.5%
Mac/PC desktops that have anti-virus software installed :	64		100%
Employees who know who their CPP Liaison is:	44		68.75%
Employees who back up all information they deem important to their work:	59		92.15%
Other Rated Security Data			
	Total #	Rating	Percent Fixed
Vulnerable computers that have been resolved (in 2002)	2		100%
Cracked passwords that have been changed (in 2002)	0		100%

INFORMATIONAL STATISTICS

Results of Questionnaire	
Employees who are known to have a security clearance :	8
Employees who answered "Yes" to the question, "Do you hold a security clearance that allows access to classified information?":	12
Proprietary Information reported in Division:	25
Personal Medical Information reported in Division:	3
Essential Systems reported in Division:	2
Required Systems reported in Division:	4
Number of employees who say they don't use a computer in the Division:	3
Other Security Data	

Thefts that have been reported in the Division (in 2002):	1
Thefts that have been reported at the Lab (in 2002):	10
Computers that have been compromised in the Division (in 2002):	1
Computers that have been compromised at the Lab (in 2002):	99
Instances of unacceptable computer use in the Division (in 2002):	5
Instances of unacceptable computer use at the Lab (in 2002):	217



INTEGRATED SAFEGUARDS & SECURITY MANAGEMENT

ERNEST ORLANDO LAWRENCE BERKELEY NATIONAL LABORATORY

Life Sciences

DIVISION INFORMATION

[ISSM Home](#)

[Take/Retake Questionnaire](#)

[Printable Questionnaire](#)

[Non-LDAP Questionnaire](#)

[View Division Profile](#) ▶

[View Division Performance](#)

[View Performance Criteria](#)

[Completed Survey](#)

[Not Completed Survey](#)

[Overview](#)

[Logout](#)

Division Director: Cooper, Priscilla K
Rubin, Edward M

ISSM Liaison: Sudar, Damir

CPP Liaison: Boswell, Martin S
Huesman, Ronald H


















Security Access Managers: Blakely, Eleanor A
Linard, Anthony M
O'Neil, James P
Rydberg, Bjorn E
Torok, Tamas

Employees in Division
([as surveyed](#)): 349

RATED STATISTICS

Click on colored square to view question and performance criteria.

Results of Survey Questions			
	Emps.	Rating	% Division Emps.
Employees in Division who have completed the Self-Assessment Questionnaire:	283		81.05%
	Emps.	Rating	% Took Survey
Classified Information reported in Division:	0		0%
UCNI reported in Division:	0		0%
NNPI reported in Division:	0		0%

Mission Critical Systems reported in Division:	0		0%
Employees who know the emergency phone number for the Laboratory :	271		95.75%
Employees who have access to the Employee Security Guide :	263		92.9%
Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building:	251		88.65%
Employees who know how to request visitor access :	275		97.15%
Employees who know whom to contact regarding keys to their office or building:	278		98.2%
Employees who take appropriate measures to secure the property assigned to them:	276		97.5%
Security Access Managers who review their access lists annually:	5		100%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues :	223		78.8%
Employees who know LBNL's legal requirements for obtaining software:	249		90.2%
Employees who have warning banners on all computers they are responsible for:	228		83.8%
Employees who change their passwords according to the LBNL password policy :	239		86.9%
Mac/PC desktops that have anti-virus software installed :	258		94.5%
Employees who know who their CPP Liaison is:	215		78.75%
Employees who back up all information they deem important to their work:	255		93.05%
Other Rated Security Data			
	Total #	Rating	Percent Fixed
Vulnerable computers that have been resolved (in 2002)	281		100%
Cracked passwords that have been changed (in 2002)	29		100%

INFORMATIONAL STATISTICS

Results of Questionnaire	
Employees who are known to have a security clearance :	0
Employees who answered "Yes" to the question, "Do you hold a security clearance that allows access to classified information?":	8
Proprietary Information reported in Division:	37
Personal Medical Information reported in Division:	21
Essential Systems reported in Division:	6

Required Systems reported in Division:	10
Number of employees who say they don't use a computer in the Division:	11
Other Security Data	
Thefts that have been reported in the Division (in 2002):	1
Thefts that have been reported at the Lab (in 2002):	10
Computers that have been compromised in the Division (in 2002):	5
Computers that have been compromised at the Lab (in 2002):	99
Instances of unacceptable computer use in the Division (in 2002):	22
Instances of unacceptable computer use at the Lab (in 2002):	217



INTEGRATED SAFEGUARDS & SECURITY MANAGEMENT

ERNEST ORLANDO LAWRENCE BERKELEY NATIONAL LABORATORY

Materials Sciences

DIVISION INFORMATION

ISSM Home

Take/Retake Questionnaire

Printable Questionnaire

Non-LDAP Questionnaire

View Division Profile ▶

View Division Performance

View Performance Criteria

Completed Survey

Not Completed Survey

Overview

Logout

Division Director: Alivisatos, A Paul
Chemla, Daniel S

ISSM Liaison: Ager, Joel W

CPP Liaison: Van Hove, Michel A

















Security Access Managers: Cavlina, Jane L
Knight, James W
Pettit, Robert S
Saiz, Eduardo

Employees in Division
([as surveyed](#)): 259

RATED STATISTICS

Click on colored square to view question and performance criteria.

Results of Survey Questions			
	Emps.	Rating	% Division Emps.
Employees in Division who have completed the Self-Assessment Questionnaire:	223		86.1%
	Emps.	Rating	% Took Survey
Classified Information reported in Division:	0		0%
UCNI reported in Division:	0		0%
NNPI reported in Division:	0		0%
Mission Critical Systems reported in Division:	0		0%

Employees who know the emergency phone number for the Laboratory :	209		93.7%
Employees who have access to the Employee Security Guide :	200		89.65%
Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building:	183		82.05%
Employees who know how to request visitor access :	204		91.45%
Employees who know whom to contact regarding keys to their office or building:	215		96.4%
Employees who take appropriate measures to secure the property assigned to them:	219		98.2%
Security Access Managers who review their access lists annually:	4		100%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues :	160		71.75%
Employees who know LBNL's legal requirements for obtaining software:	193		89.75%
Employees who have warning banners on all computers they are responsible for:	163		77.25%
Employees who change their passwords according to the LBNL password policy :	176		83.4%
Mac/PC desktops that have anti-virus software installed :	204		95.75%
Employees who know who their CPP Liaison is:	158		74.5%
Employees who back up all information they deem important to their work:	208		96.7%
Other Rated Security Data			
	Total #	Rating	Percent Fixed
Vulnerable computers that have been resolved (in 2002)	131		98%
Cracked passwords that have been changed (in 2002)	16		100%

INFORMATIONAL STATISTICS

Results of Questionnaire	
Employees who are known to have a security clearance :	2
Employees who answered "Yes" to the question, "Do you hold a security clearance that allows access to classified information?":	12
Proprietary Information reported in Division:	25
Personal Medical Information reported in Division:	3
Essential Systems reported in Division:	0
Required Systems reported in Division:	0

Number of employees who say they don't use a computer in the Division:	13
Other Security Data	
Thefts that have been reported in the Division (in 2002):	0
Thefts that have been reported at the Lab (in 2002):	10
Computers that have been compromised in the Division (in 2002):	10
Computers that have been compromised at the Lab (in 2002):	99
Instances of unacceptable computer use in the Division (in 2002):	28
Instances of unacceptable computer use at the Lab (in 2002):	217



INTEGRATED SAFEGUARDS & SECURITY MANAGEMENT

ERNEST ORLANDO LAWRENCE BERKELEY NATIONAL LABORATORY

NERSC

DIVISION INFORMATION

ISSM Home

Take/Retake Questionnaire

Printable Questionnaire

Non-LDAP Questionnaire

View Division Profile ▶

View Division Performance

View Performance Criteria

Completed Survey

Not Completed Survey

Overview

Logout

Division Director: Simon, Horst D

ISSM Liaison: Ramsey, Dwayne

CPP Liaison: Campbell, Scott
Lau Jr, Stephen















Security Access Managers: Dooly, Martin K

Employees in Division
([as surveyed](#)): 188

RATED STATISTICS

Click on colored square to view question and performance criteria.

Results of Survey Questions			
	Emps.	Rating	% Division Emps.
Employees in Division who have completed the Self-Assessment Questionnaire:	158		84%
	Emps.	Rating	% Took Survey
Classified Information reported in Division:	0		0%
UCNI reported in Division:	0		0%
NNPI reported in Division:	0		0%
Mission Critical Systems reported in Division:	0		0%
Employees who know the emergency phone number for the Laboratory :	154		97.45%
Employees who have access to the Employee Security Guide :	146		92.4%

Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building:	134		84.8%
Employees who know how to request visitor access :	147		93%
Employees who know whom to contact regarding keys to their office or building:	151		95.55%
Employees who take appropriate measures to secure the property assigned to them:	157		99.35%
Security Access Managers who review their access lists annually:	1		100%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues :	117		74.05%
Employees who know LBNL's legal requirements for obtaining software:	146		92.95%
Employees who have warning banners on all computers they are responsible for:	148		93.65%
Employees who change their passwords according to the LBNL password policy :	157		99.35%
Mac/PC desktops that have anti-virus software installed :	143		95.95%
Employees who know who their CPP Liaison is:	134		84.8%
Employees who back up all information they deem important to their work:	154		97.45%
Other Rated Security Data			
	Total #	Rating	Percent Fixed
Vulnerable computers that have been resolved (in 2002)	278		99%
Cracked passwords that have been changed (in 2002)	3		100%

INFORMATIONAL STATISTICS

Results of Questionnaire	
Employees who are known to have a security clearance :	8
Employees who answered "Yes" to the question, "Do you hold a security clearance that allows access to classified information?":	7
Proprietary Information reported in Division:	32
Personal Medical Information reported in Division:	0
Essential Systems reported in Division:	3
Required Systems reported in Division:	5
Number of employees who say they don't use a computer in the Division:	9
Other Security Data	

Thefts that have been reported in the Division (in 2002):	2
Thefts that have been reported at the Lab (in 2002):	10
Computers that have been compromised in the Division (in 2002):	8
Computers that have been compromised at the Lab (in 2002):	99
Instances of unacceptable computer use in the Division (in 2002):	13
Instances of unacceptable computer use at the Lab (in 2002):	217



INTEGRATED SAFEGUARDS & SECURITY MANAGEMENT

ERNEST ORLANDO LAWRENCE BERKELEY NATIONAL LABORATORY

Nuclear Science

DIVISION INFORMATION

[ISSM Home](#)

[Take/Retake Questionnaire](#)

[Printable Questionnaire](#)

[Non-LDAP Questionnaire](#)

[View Division Profile](#) ▶

[View Division Performance](#)

[View Performance Criteria](#)

[Completed Survey](#)

[Not Completed Survey](#)

[Overview](#)

[Logout](#)

Division Director: Schroeder, Lee S
Symons, Timothy J

ISSM Liaison: Freeman, John C

CPP Liaison: Matis, Howard S
















Security Access Managers: Kono, Joy N
Norris, Margaret A

Employees in Division
([as surveyed](#)): 134

RATED STATISTICS

Click on colored square to view question and performance criteria.

Results of Survey Questions			
	Emps.	Rating	% Division Emps.
Employees in Division who have completed the Self-Assessment Questionnaire:	128		95.5%
	Emps.	Rating	% Took Survey
Classified Information reported in Division:	0		0%
UCNI reported in Division:	0		0%
NNPI reported in Division:	0		0%
Mission Critical Systems reported in Division:	0		0%
Employees who know the emergency phone number for the Laboratory :	121		94.5%

Employees who have access to the Employee Security Guide :	116		90.6%
Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building:	109		85.15%
Employees who know how to request visitor access :	115		89.8%
Employees who know whom to contact regarding keys to their office or building:	122		95.3%
Employees who take appropriate measures to secure the property assigned to them:	124		96.85%
Security Access Managers who review their access lists annually:	2		100%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues :	102		79.65%
Employees who know LBNL's legal requirements for obtaining software:	109		88.6%
Employees who have warning banners on all computers they are responsible for:	105		85.35%
Employees who change their passwords according to the LBNL password policy :	100		80%
Mac/PC desktops that have anti-virus software installed :	104		87.35%
Employees who know who their CPP Liaison is:	96		78.05%
Employees who back up all information they deem important to their work:	114		91.9%
Other Rated Security Data			
	Total #	Rating	Percent Fixed
Vulnerable computers that have been resolved (in 2002)	73		100%
Cracked passwords that have been changed (in 2002)	4		100%

INFORMATIONAL STATISTICS

Results of Questionnaire	
Employees who are known to have a security clearance :	1
Employees who answered "Yes" to the question, "Do you hold a security clearance that allows access to classified information?":	10
Proprietary Information reported in Division:	1
Personal Medical Information reported in Division:	0
Essential Systems reported in Division:	4
Required Systems reported in Division:	5
Number of employees who say they don't use a computer in the Division:	10

Other Security Data	
Thefts that have been reported in the Division (in 2002):	0
Thefts that have been reported at the Lab (in 2002):	10
Computers that have been compromised in the Division (in 2002):	4
Computers that have been compromised at the Lab (in 2002):	99
Instances of unacceptable computer use in the Division (in 2002):	8
Instances of unacceptable computer use at the Lab (in 2002):	217



INTEGRATED SAFEGUARDS & SECURITY MANAGEMENT

ERNEST ORLANDO LAWRENCE BERKELEY NATIONAL LABORATORY

Operations

DIVISION INFORMATION

ISSM Home

Take/Retake Questionnaire

Printable Questionnaire

Non-LDAP Questionnaire

View Division Profile ▶

View Division Performance

View Performance Criteria

Completed Survey

Not Completed Survey

Overview

Logout

Division Director: Benson, Sally M

ISSM Liaison: Bear, Guy

CPP Liaison: None identified















Security Access Managers: Kolandaisamy, Edna P

Employees in Division
([as surveyed](#)): 18

RATED STATISTICS

Click on colored square to view question and performance criteria.

Results of Survey Questions			
	Emps.	Rating	% Division Emps.
Employees in Division who have completed the Self-Assessment Questionnaire:	15		83.3%
	Emps.	Rating	% Took Survey
Classified Information reported in Division:	0		0%
UCNI reported in Division:	0		0%
NNPI reported in Division:	0		0%
Mission Critical Systems reported in Division:	0		0%
Employees who know the emergency phone number for the Laboratory :	15		100%
Employees who have access to the Employee Security Guide :	15		100%
Employees who know how to find the list of building authorizers if access is required to			

a proximity card-enabled building:	13		86.65%
Employees who know how to request visitor access :	14		93.3%
Employees who know whom to contact regarding keys to their office or building:	15		100%
Employees who take appropriate measures to secure the property assigned to them:	15		100%
Security Access Managers who review their access lists annually:	1		100%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues :	13		86.65%
Employees who know LBNL's legal requirements for obtaining software:	13		86.65%
Employees who have warning banners on all computers they are responsible for:	14		93.3%
Employees who change their passwords according to the LBNL password policy :	15		100%
Mac/PC desktops that have anti-virus software installed :	15		100%
Employees who know who their CPP Liaison is:	14		93.3%
Employees who back up all information they deem important to their work:	15		100%
Other Rated Security Data			
	Total #	Rating	Percent Fixed
Vulnerable computers that have been resolved (in 2002)	0		100%
Cracked passwords that have been changed (in 2002)	0		100%

INFORMATIONAL STATISTICS

Results of Questionnaire	
Employees who are known to have a security clearance :	0
Employees who answered "Yes" to the question, "Do you hold a security clearance that allows access to classified information?":	0
Proprietary Information reported in Division:	2
Personal Medical Information reported in Division:	0
Essential Systems reported in Division:	1
Required Systems reported in Division:	2
Number of employees who say they don't use a computer in the Division:	0
Other Security Data	
Thefts that have been reported in the Division (in 2002):	0

Thefts that have been reported at the Lab (in 2002):	10
Computers that have been compromised in the Division (in 2002):	0
Computers that have been compromised at the Lab (in 2002):	99
Instances of unacceptable computer use in the Division (in 2002):	0
Instances of unacceptable computer use at the Lab (in 2002):	217



INTEGRATED SAFEGUARDS & SECURITY MANAGEMENT

ERNEST ORLANDO LAWRENCE BERKELEY NATIONAL LABORATORY

Physical Biosciences

DIVISION INFORMATION

ISSM Home

Take/Retake Questionnaire

Printable Questionnaire

Non-LDAP Questionnaire

View Division Profile ▶

View Division Performance

View Performance Criteria

Completed Survey

Not Completed Survey

Overview

Logout

Division Director: Fleming, Graham R

ISSM Liaison: Pelton, Jeffrey G

CPP Liaison: Grosse-Kunstleve, Ralf Wilhelm

Security Access Managers: Berry, Edward A

Ford, Ellen

Pettit, Robert S
















Williams, Philip G

Employees in Division
([as surveyed](#)): 135

RATED STATISTICS

Click on colored square to view question and performance criteria.

Results of Survey Questions			
	Emps.	Rating	% Division Emps.
Employees in Division who have completed the Self-Assessment Questionnaire:	97		71.85%
	Emps.	Rating	% Took Survey
Classified Information reported in Division:	0		0%
UCNI reported in Division:	0		0%
NNPI reported in Division:	0		0%
Mission Critical Systems reported in Division:	0		0%
Employees who know the emergency phone number for the Laboratory :	92		94.85%

Employees who have access to the Employee Security Guide :	83		85.55%
Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building:	78		80.4%
Employees who know how to request visitor access :	89		91.75%
Employees who know whom to contact regarding keys to their office or building:	94		96.9%
Employees who take appropriate measures to secure the property assigned to them:	95		97.9%
Security Access Managers who review their access lists annually:	4		100%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues :	71		73.2%
Employees who know LBNL's legal requirements for obtaining software:	82		86.3%
Employees who have warning banners on all computers they are responsible for:	76		80.85%
Employees who change their passwords according to the LBNL password policy :	83		87.35%
Mac/PC desktops that have anti-virus software installed :	88		94.6%
Employees who know who their CPP Liaison is:	76		80%
Employees who back up all information they deem important to their work:	90		93.75%
Other Rated Security Data			
	Total #	Rating	Percent Fixed
Vulnerable computers that have been resolved (in 2002)	124		100%
Cracked passwords that have been changed (in 2002)	14		100%

INFORMATIONAL STATISTICS

Results of Questionnaire	
Employees who are known to have a security clearance :	0
Employees who answered "Yes" to the question, "Do you hold a security clearance that allows access to classified information?":	1
Proprietary Information reported in Division:	8
Personal Medical Information reported in Division:	0
Essential Systems reported in Division:	0
Required Systems reported in Division:	1
Number of employees who say they don't use a computer in the Division:	5

Other Security Data	
Thefts that have been reported in the Division (in 2002):	0
Thefts that have been reported at the Lab (in 2002):	10
Computers that have been compromised in the Division (in 2002):	2
Computers that have been compromised at the Lab (in 2002):	99
Instances of unacceptable computer use in the Division (in 2002):	4
Instances of unacceptable computer use at the Lab (in 2002):	217



INTEGRATED SAFEGUARDS & SECURITY MANAGEMENT

ERNEST ORLANDO LAWRENCE BERKELEY NATIONAL LABORATORY

Physics

DIVISION INFORMATION

ISSM Home

Take/Retake Questionnaire

Printable Questionnaire

Non-LDAP Questionnaire

View Division Profile ▶

View Division Performance

View Performance Criteria

Completed Survey

Not Completed Survey

Overview

Logout

Division Director: Siegrist, James L

ISSM Liaison: Freeman, John C

CPP Liaison: Ciocio, Alessandra















Security Access Managers: Kono, Joy N

Employees in Division
([as surveyed](#)): 163

RATED STATISTICS

Click on colored square to view question and performance criteria.

Results of Survey Questions			
	Emps.	Rating	% Division Emps.
Employees in Division who have completed the Self-Assessment Questionnaire:	142		87.1%
	Emps.	Rating	% Took Survey
Classified Information reported in Division:	0		0%
UCNI reported in Division:	0		0%
NNPI reported in Division:	0		0%
Mission Critical Systems reported in Division:	0		0%
Employees who know the emergency phone number for the Laboratory :	130		91.55%
Employees who have access to the Employee Security Guide :	127		89.4%
Employees who know how to find the list of building authorizers if access is required to			

a proximity card-enabled building:	92		64.75%
Employees who know how to request visitor access :	127		89.4%
Employees who know whom to contact regarding keys to their office or building:	135		95.05%
Employees who take appropriate measures to secure the property assigned to them:	139		97.85%
Security Access Managers who review their access lists annually:	1		100%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues :	80		56.3%
Employees who know LBNL's legal requirements for obtaining software:	115		83.3%
Employees who have warning banners on all computers they are responsible for:	114		84.4%
Employees who change their passwords according to the LBNL password policy :	124		89.85%
Mac/PC desktops that have anti-virus software installed :	113		89.65%
Employees who know who their CPP Liaison is:	102		73.9%
Employees who back up all information they deem important to their work:	130		94.2%
Other Rated Security Data			
	Total #	Rating	Percent Fixed
Vulnerable computers that have been resolved (in 2002)	133		100%
Cracked passwords that have been changed (in 2002)	0		100%

INFORMATIONAL STATISTICS

Results of Questionnaire	
Employees who are known to have a security clearance :	2
Employees who answered "Yes" to the question, "Do you hold a security clearance that allows access to classified information?":	2
Proprietary Information reported in Division:	4
Personal Medical Information reported in Division:	1
Essential Systems reported in Division:	0
Required Systems reported in Division:	0
Number of employees who say they don't use a computer in the Division:	18
Other Security Data	
Thefts that have been reported in the Division (in 2002):	0

Thefts that have been reported at the Lab (in 2002):	10
Computers that have been compromised in the Division (in 2002):	9
Computers that have been compromised at the Lab (in 2002):	99
Instances of unacceptable computer use in the Division (in 2002):	4
Instances of unacceptable computer use at the Lab (in 2002):	217

Appendix F

Institutional Profiles

Organization Performance 10/29/02

	Employees in Division who have completed the Self-Assessment Questionnaire:	Classified Information reported in Division:	UCNI reported in Division:	NNPI reported in Division:	Mission Critical Systems reported in Division:	Employees who know the emergency phone number for the Laboratory:	Employees who have access to the Employee Security Guide :	Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building:	Employees who know how to request visitor access:	Employees who know whom to contact regarding keys to their office or building:	Employees who take appropriate measures to secure the property assigned to them:	Security Access Managers who review their access lists annually:	Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues:	Employees who know LBNL's legal requirements for obtaining software:	Employees who have warning banners on all computers they are responsible for:	Employees who change their passwords according to the LBNL password policy:	Mac/PC desktops that have anti-virus software installed:	Employees who know their CPP Liaison is:	Employees who back up all information they deem important to their work:	Vulnerable computers that have been resolved	Cracked passwords that have been changed
Administrative Services	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■ (in 2002)	■ (date N/A)
Accelerator & Fusion Research	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■ (in 2002)	■ (date N/A)
Advanced Light Source	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■ (in 2002)	■ (date N/A)
Financial Services	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■ (in 2002)	■ (date N/A)
Chemical Sciences	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■ (in 2002)	■ (date N/A)
Computing Sciences	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■ (in 2002)	■ (date N/A)
Environmental Energy Tech.	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■ (in 2002)	■ (date N/A)
Engineering	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■ (in 2002)	■ (date N/A)
Environment, Health & Safety	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■ (in 2002)	■ (date N/A)
Earth Sciences	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■ (in 2002)	■ (date N/A)
Facilities	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■ (in 2002)	■ (date N/A)
Genomics Division	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■ (in 2002)	■ (date N/A)
Human Resources	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■ (in 2002)	■ (date N/A)
Info, Technologies & Services	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■ (in 2002)	■ (date N/A)
Laboratory Directorate	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■ (in 2002)	■ (date N/A)
Life Sciences	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■ (in 2002)	■ (date N/A)
Materials Sciences	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■ (in 2002)	■ (date N/A)
NERSC	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■ (in 2002)	■ (date N/A)
Nuclear Science	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■ (in 2002)	■ (date N/A)
Operations	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■ (in 2002)	■ (date N/A)
Physical Biosciences	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■ (in 2002)	■ (date N/A)
Physics	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■ (in 2002)	■ (date N/A)

Organization Performance 2/19/03

	Employees in Division who have completed the Self-Assessment Questionnaire:	Classified Information reported in Division:	UCNI reported in Division:	NNPI reported in Division:	Mission Critical Systems reported in Division:	Employees who know the emergency phone number for the Laboratory :	Employees who have access to the Employee Security Guide :	Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building:	Employees who know how to request visitor access :	Employees who know whom to contact regarding keys to their office or building:	Employees who take appropriate measures to secure the property assigned to them:	Security Access Managers who review their access lists annually:	Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues :	Employees who know LBNL's legal requirements for obtaining software:	Employees who have warning banners on all computers they are responsible for:	Employees who change their passwords according to the LBNL password policy :	Mac/PC desktops that have anti-virus software installed:	Employees who know their CPP Liaison is:	Employees who back up all information they deem important to their work:	Vulnerable computers that have been resolved	Cracked passwords that have been changed
Administrative Services	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div> (in 2002)	<div></div> (in 2002)
Accelerator & Fusion Research	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div> (in 2002)	<div></div> (in 2002)
Advanced Light Source	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div> (in 2002)	<div></div> (in 2002)
Financial Services	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div> (in 2002)	<div></div> (in 2002)
Chemical Sciences	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div> (in 2002)	<div></div> (in 2002)
Computing Sciences	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div> (in 2002)	<div></div> (in 2002)
Environmental Energy Tech.	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div> (in 2002)	<div></div> (in 2002)
Engineering	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div> (in 2002)	<div></div> (in 2002)
Environment, Health & Safety	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div> (in 2002)	<div></div> (in 2002)
Earth Sciences	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div> (in 2002)	<div></div> (in 2002)
Facilities	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div> (in 2002)	<div></div> (in 2002)
Genomics Division	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div> (in 2002)	<div></div> (in 2002)
Human Resources	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div> (in 2002)	<div></div> (in 2002)
Info. Technologies & Services	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div> (in 2002)	<div></div> (in 2002)
Laboratory Directorate	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div> (in 2002)	<div></div> (in 2002)
Life Sciences	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div> (in 2002)	<div></div> (in 2002)
Materials Sciences	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div> (in 2002)	<div></div> (in 2002)
NERSC	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div> (in 2002)	<div></div> (in 2002)
Nuclear Science	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div> (in 2002)	<div></div> (in 2002)
Operations	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div> (in 2002)	<div></div> (in 2002)
Physical Biosciences	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div> (in 2002)	<div></div> (in 2002)
Physics	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div> (in 2002)	<div></div> (in 2002)

DISCLAIMER

This document was prepared as an account of work sponsored by the United States Government. While this document is believed to contain correct information, neither the United States Government nor any agency thereof, nor The Regents of the University of California, nor any of their employees, makes any warranty, express or implied, or assumes any legal responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by its trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or The Regents of the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof or The Regents of the University of California.